BlackBerry Enterprise Server for Microsoft Exchange

Version: 5.0

Feature and Technical Overview

BlackBerry

SWDT305802-524791-0331031644-001

Contents

1 Overview: BlackBerry Enterprise Server 5
New in this release 5

2 BlackBerry Enterprise Server architecture 11
Architecture: BlackBerry Enterprise Server 11
Architecture: Remote BlackBerry Collaboration Service 16
Architecture: Remote BlackBerry MDS Connection Service 17
Architecture: Remote BlackBerry MDS Integration Service 19
Architecture: Remote BlackBerry Router 20
Architecture: Remote BlackBerry Administration Service 21
Architecture: Remote BlackBerry Monitoring Service 23
Architecture: Remote BlackBerry Attachment Service 24
Architecture: BlackBerry Web Desktop Manager 26

3 BlackBerry Enterprise Server components and features 27
BlackBerry messaging and collaboration services 27
BlackBerry Messaging Agent 27
BlackBerry Collaboration Service 31
BlackBerry Synchronization Service 33
BlackBerry Attachment Service 35
BlackBerry MDS 36
BlackBerry Applications 37
BlackBerry MDS Connection Service 39
BlackBerry MDS Integration Service 40
Managing BlackBerry Java Applications and BlackBerry Device Software 41
BlackBerry MDS Application Console 42
BlackBerry device management 42
Controlling third-party applications on BlackBerry devices 43
BlackBerry Enterprise Solution security 43
Master encryption keys 44
Standard BlackBerry encryption 44
Options for extending messaging security 45
Options for encrypting stored data 46
Controlling BlackBerry device access to the BlackBerry Enterprise Server 47

Managing BlackBerry device security over the wireless network using IT administration commands ... 48
BlackBerry Monitoring Service ... 48
BlackBerry Threshold Analysis Tool ... 50
BlackBerry Router ... 51
BlackBerry Policy Service ... 51
BlackBerry Configuration Panel ... 52
BlackBerry Administration Service ... 52
BlackBerry Web Desktop Manager ... 53
Comparison of BlackBerry Web Desktop Manager and BlackBerry Desktop Manager features ... 55

4 BlackBerry Enterprise Server high availability ... 59
BlackBerry Enterprise Server high availability in a small-scale environment ... 59
How the BlackBerry Enterprise Server calculates health scores ... 60
Conditions for failover to a standby BlackBerry Enterprise Server ... 60
How a primary BlackBerry Enterprise Server demotes itself ... 61
Scenario: What happens after a primary BlackBerry Enterprise Server stops responding ... 61
Scenario: What happens after the health score of a primary BlackBerry Enterprise Server falls below the failover threshold ... 62
BlackBerry Configuration Database high availability ... 62
BlackBerry Configuration Database mirroring ... 63
Scenario: What happens after the principal BlackBerry Configuration Database stops responding ... 63
High availability in a distributed environment ... 64

5 BlackBerry Enterprise Server process flows ... 67
Messaging process flows ... 67
Process flow: Sending a message to a BlackBerry device ... 67
Process flow: Sending a message from a BlackBerry device ... 68
Process flow: Sending a message that contains an attachment from a BlackBerry device ... 68
Process flow: Searching an organization's address book from a BlackBerry device ... 70
Instant messaging process flows ... 71
Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Live Communications Server 2005 (Microsoft Office Communicator) ... 71
Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Communications Server 2007 ... 72
Process flow: Starting an instant messaging session using the BlackBerry Client for IBM Lotus Sametime ... 74

Process flow: Starting an instant messaging session using the BlackBerry Client for Novell GroupWise Messenger 75
Process flow: Sending a file to a contact using the BlackBerry Client for IBM Lotus Sametime 76
Message attachment process flows 78
Process flow: Viewing a message attachment 78
Process flow: Viewing an attachment using a link 79
Organizer data process flows 80
Process flow: Synchronizing organizer data for the first time on a BlackBerry device 80
Process flow: Synchronizing subsequent changes to organizer data 81
Process flow: Adding a contact picture on a BlackBerry device 82
Mobile data process flows 83
Process flow: Requesting BlackBerry Browser content on a BlackBerry device 83
Process flow: Requesting BlackBerry Browser content while access control is turned on for the BlackBerry MDS Connection Service 84
Process flow: Requesting BlackBerry Browser content with two-factor authentication turned on 85
Process flow: Pushing application content to a BlackBerry device 86
Process flow: Installing a BlackBerry Java Application on a BlackBerry device over the wireless network 87
Process flow: Installing a BlackBerry MDS Runtime Application on a BlackBerry device over the wireless network 89
Process flow: Installing a BlackBerry Browser Application on a BlackBerry device over the wireless network 90
BlackBerry device management process flows 91
Process flow: Activating a BlackBerry device over the wireless network 91
Process flow: Resending an IT policy to a BlackBerry device manually 92
Process flow: Authenticating data on a BlackBerry device without connecting to the BlackBerry Infrastructure 92
Monitoring process flows 93
Process flow: Updating and displaying data in the BlackBerry Monitoring Service console 93
Process flow: Storing data in the BlackBerry Monitoring Service database 93

6 Wi-Fi enabled BlackBerry devices 94
Types of Wi-Fi networks 94
Wireless access points 95
BlackBerry Enterprise Server support for Wi-Fi enabled BlackBerry devices 96
Connections that BlackBerry devices make to mobile and Wi-Fi networks 97
Connecting Wi-Fi enabled BlackBerry devices to the BlackBerry Enterprise Server over a Wi-Fi connection 99

Direct connections between BlackBerry devices and the BlackBerry Router over an enterprise Wi-Fi network..... 99
Wi-Fi connection when a VPN connection or direct connection between BlackBerry devices and the BlackBerry Router is not possible..... 99
Priority for connections that BlackBerry devices make over a Wi-Fi network..... 100
BlackBerry services that are available over Wi-Fi connections..... 100
IEEE 802.11 wireless networking standards that Wi-Fi enabled BlackBerry devices support..... 103
Characteristics of the IEEE 802.11a wireless networking standard that Wi-Fi enabled BlackBerry devices support 103
Characteristics of the IEEE 802.11b wireless networking standard that Wi-Fi enabled BlackBerry devices support 103
Characteristics of the IEEE 802.11g wireless networking standard that Wi-Fi enabled BlackBerry devices support 104

7 Glossary..... 105

8 Provide feedback..... 109

9 Legal notice..... 110

Overview: BlackBerry Enterprise Server

1

The BlackBerry® Enterprise Server is designed to be a secure, centralized link between an organization's wireless network, communications software, applications, and BlackBerry devices. The BlackBerry Enterprise Server integrates with your organization's existing infrastructure, which can include messaging and collaboration software, calendar and contact information, wireless Internet and intranet access, and custom applications, to provide BlackBerry device users with mobile access to your organization's resources.

The BlackBerry Enterprise Server supports AES and Triple DES encryption to protect and ensure the integrity of wireless data that is transmitted between the BlackBerry Enterprise Server components and BlackBerry devices. You can select from more than 450 IT policy rules that you can configure to control the features of the BlackBerry devices that are used in your organization's environment.

The BlackBerry Enterprise Server supports several optional components and configurations to meet your organization's requirements. The BlackBerry Collaboration Service integrates with supported third-party instant messaging servers to permit users to access your organization's instant messaging system from their BlackBerry devices using the BlackBerry instant messaging client. The BlackBerry MDS Integration Service supports custom application development and distribution. You can configure the BlackBerry Enterprise Server and the BlackBerry Enterprise Server components to support high availability to enhance the consistency and reliability of your organization's environment.

You can manage the BlackBerry Enterprise Server, BlackBerry devices, and user accounts using the BlackBerry Administration Service, a web application that is accessible from any computer that can access to the computer that hosts the BlackBerry Administration Service. You can use the BlackBerry Administration Service to manage a BlackBerry Domain, which consists of multiple BlackBerry Enterprise Server instances that use a single BlackBerry Configuration Database.

New in this release

Feature	Description
BlackBerry® Administration Service	The BlackBerry Administration Service is a web application that connects to the BlackBerry Configuration Database. You can use the BlackBerry Administration Service to manage the BlackBerry Domain, which includes user accounts and features that you can use to control BlackBerry devices. The BlackBerry Domain consists of a single BlackBerry Configuration Database and all of the BlackBerry® Enterprise Server instances that use it. The BlackBerry Administration Service replaces the BlackBerry Manager as the administration console for the BlackBerry Enterprise Server and BlackBerry Enterprise Server components.

Feature	Description
BlackBerry® Web Desktop Manager	The BlackBerry Web Desktop Manager is a web application that permits users to manage their BlackBerry devices. For example, users can activate BlackBerry devices, back up and restore data, select messaging options, and synchronize data. The BlackBerry Web Desktop Manager includes the BlackBerry® Device Manager.
BlackBerry Enterprise Server high availability	BlackBerry Enterprise Server high availability consists of a minimum of two BlackBerry Enterprise Server instances and the BlackBerry Configuration Database replicated across two database servers. High availability is designed so that no single point of failure exists in the BlackBerry® Enterprise Solution that could stop the messaging and application data flow to and from BlackBerry devices.
High availability for a distributed environment	If you install multiple BlackBerry Enterprise Server components on different computers to create a distributed environment, you can configure the components for high availability. High availability for a distributed component requires that you install two or more instances of the component in your organization's environment. When an instance stops responding, the other instances can take over.
Support for database mirroring	If your organization uses Microsoft® SQL Server® 2005 SP2 or later, you can configure database mirroring. Database mirroring requires a principal database, mirror database, and, optionally, a witness. Although the BlackBerry Enterprise Server can contact the mirror database, it opens active connections to the principal database only. If the principal database stops responding, the BlackBerry Enterprise Server opens an active connection to the mirror database automatically. Database mirroring provides fault tolerance for the BlackBerry Enterprise Solution.
Support for Microsoft SQL Server 2005 Express Edition	BlackBerry Enterprise Server version 5.0 supports Microsoft SQL Server 2005 Express Edition. The setup application can install Microsoft SQL Server 2005 Express Edition if your organization's environment does not already include a database server.
Support for Windows Server® 2008	BlackBerry Enterprise Server version 5.0 supports Windows Server 2008.
Enrolling certificates over the wireless network	You can configure the BlackBerry Enterprise Server to permit BlackBerry devices to enroll certificates over the wireless network. Permitting BlackBerry devices to enroll certificates is an alternative to instructing users to send the certificates to themselves in an email message or using the certificate synchronization tool in the BlackBerry® Desktop Software.

Feature	Description
New method for installing and managing the BlackBerry® Device Software and BlackBerry Java® Applications	You can use the BlackBerry Administration Service to install and manage the BlackBerry Device Software and BlackBerry Java Applications on BlackBerry devices. In the BlackBerry Administration Service, you create software configurations to specify the versions of the BlackBerry Device Software and BlackBerry Java Applications that you want to install or update on BlackBerry devices, or remove from BlackBerry devices. You also use software configurations to specify which applications are required, optional, or not permitted on BlackBerry devices. When you create a software configuration, you must also specify whether users can install applications that are not listed in the software configuration on their BlackBerry devices. When you add a BlackBerry Java Application to a software configuration, you must assign an application control policy to the application to specify what resources the application can access on BlackBerry devices. If you permit users to install unlisted applications, you must create an application control policy for unlisted applications that specifies what resources the applications can access on BlackBerry devices. If you assign more than one software configuration to a user account, all of the settings in the multiple software configurations are applied to the BlackBerry device. The BlackBerry Enterprise Server resolves conflicting settings using predefined reconciliation rules and prioritized rankings that you can specify using the BlackBerry Administration Service. For more information about installing and managing the BlackBerry Device Software on BlackBerry devices, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Device Software Update Guide*.
BlackBerry® MDS Application Console	The BlackBerry MDS Application Console is a web-based administration console that you can use to manage BlackBerry® MDS Runtime Applications and BlackBerry Browser Applications that reside in the BlackBerry MDS Application Repository. You can use the BlackBerry MDS Application Console to send requests to a BlackBerry MDS Integration Service to install or update BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on BlackBerry devices, or to remove the applications from BlackBerry devices. You install the BlackBerry MDS Application Console when you install the BlackBerry MDS Integration Service.

Feature	Description
	The BlackBerry MDS Application Console supports BlackBerry MDS Integration Service version 5.0 or later.
Support for new BlackBerry® Browser Applications	BlackBerry Enterprise Server version 5.0 supports the following types of BlackBerry Browser Applications: • browser channel push applications: An icon displays on the Home screens of BlackBerry devices to indicate whether users viewed the latest version of the web content that the Browser Push Engine pushed to the BlackBerry devices. • browser cache push applications: The Browser Push Engine pushes web content to the cache of the BlackBerry Browser on BlackBerry devices. To view the web content, users browse to the appropriate web address using the BlackBerry Browser. • browser message push applications: A message appears in the message list on BlackBerry devices to provide a link to new or updated web content. For more information about developing and customizing BlackBerry Applications, visit www.blackberry.com/developers.
Follow-up flag on email messages	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can flag email messages on their BlackBerry devices and set reminder times.
Forward calendar entries	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can forward meeting invitations and calendar entries from their BlackBerry devices.
Manage personal folders	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can add, delete, move, and rename personal folders from their BlackBerry devices.
View and manage personal contact subfolders	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can view personal contact subfolders on their BlackBerry devices and change contact information. Users can specify which contact subfolders that they want to synchronize to their BlackBerry devices using the BlackBerry® Desktop Manager or BlackBerry Web Desktop Manager. You can limit the number of contact subfolders that users can synchronize to their BlackBerry devices.

Feature	Description
View and use contacts in public folders	Users with BlackBerry Device Software version 5.0 or later can view and use contacts in public folders from their BlackBerry devices, and copy the contacts to their contact lists. Users can only view the public folders that they have the appropriate permissions for. Users can specify which public folders they want to synchronize to their BlackBerry devices using the BlackBerry Desktop Manager or BlackBerry Web Desktop Manager. You can limit the number of public folders that users can synchronize to their BlackBerry devices.
Attachment support for the .wma file format	The BlackBerry Attachment Service now supports the .wma audio file format.
New IT policy rules	For information about new IT policy groups and IT policy rules, visit www.blackberry.com/go/serverdocs to see the *Policy Reference Guide*.
Changes to the BlackBerry Configuration Database schema	BlackBerry Enterprise Server version 5.0 contains changes to the BlackBerry Configuration Database schema. The changes occur in the following files: • 4.5\UpgradeV20070831.sql • 4.5\UpgradeV20071010.sql • 4.5\UpgradeV20071030.sql • 4.5\UpgradeV20080715.sql • 5.0\UpgradeV20090122.sql • 5.0\UpgradeV99990101.sql

BlackBerry Monitoring Service

Feature	Description
Monitor up to 57 weeks of data	The BlackBerry Monitoring Service saves data for BlackBerry Enterprise Server components from the previous 57 weeks. The additional historical data can be useful if you generate a chart to view the activity of a BlackBerry Enterprise Server component over time.
Monitor a data attribute of BlackBerry Enterprise Server components or BlackBerry device users by rate	The BlackBerry Monitoring Service console displays statistics according to the level of activity over a specific period of time for specific data attributes of BlackBerry Enterprise Server components and BlackBerry device users. For example, the BlackBerry Monitoring Service console displays the number of messages sent to BlackBerry device users per hour.

Feature	Description
Monitor the connection status of BlackBerry Enterprise Server components	The BlackBerry Monitoring Service monitors the connection status of many BlackBerry Enterprise Server components, including connections to the BlackBerry Configuration Database, BlackBerry Messaging Agent, BlackBerry Controller, and BlackBerry Router. The BlackBerry Monitoring Service also monitors the connection status of the SRP connection for a component.
Generate appropriate thresholds that you can use to monitor BlackBerry Enterprise Server components and BlackBerry device users automatically	The BlackBerry Threshold Analysis Tool is designed to determine appropriate thresholds that you can use to monitor data-attributes of BlackBerry Enterprise Server components and BlackBerry device users. Instead of defining thresholds in the BlackBerry Monitoring Service console manually, you can run the BlackBerry Threshold Analysis Tool and define thresholds that are designed to monitor irregular levels of activity automatically.
Monitor remote BlackBerry Enterprise Server components	The BlackBerry Monitoring Service monitors remote BlackBerry Enterprise Server components.
Specify maintenance windows for thresholds or BlackBerry Enterprise Server instances	You can use the BlackBerry Monitoring Service console to schedule regular and temporary maintenance windows for thresholds and BlackBerry Enterprise Server instances. The BlackBerry Monitoring Service does not monitor BlackBerry Enterprise Server instances or thresholds during maintenance windows.
View diagnostic information for BlackBerry devices in the BlackBerry Monitoring Service console	You can use the BlackBerry Monitoring Service console to request and view diagnostic information for BlackBerry devices that are running BlackBerry Device Software version 5.0 or later.

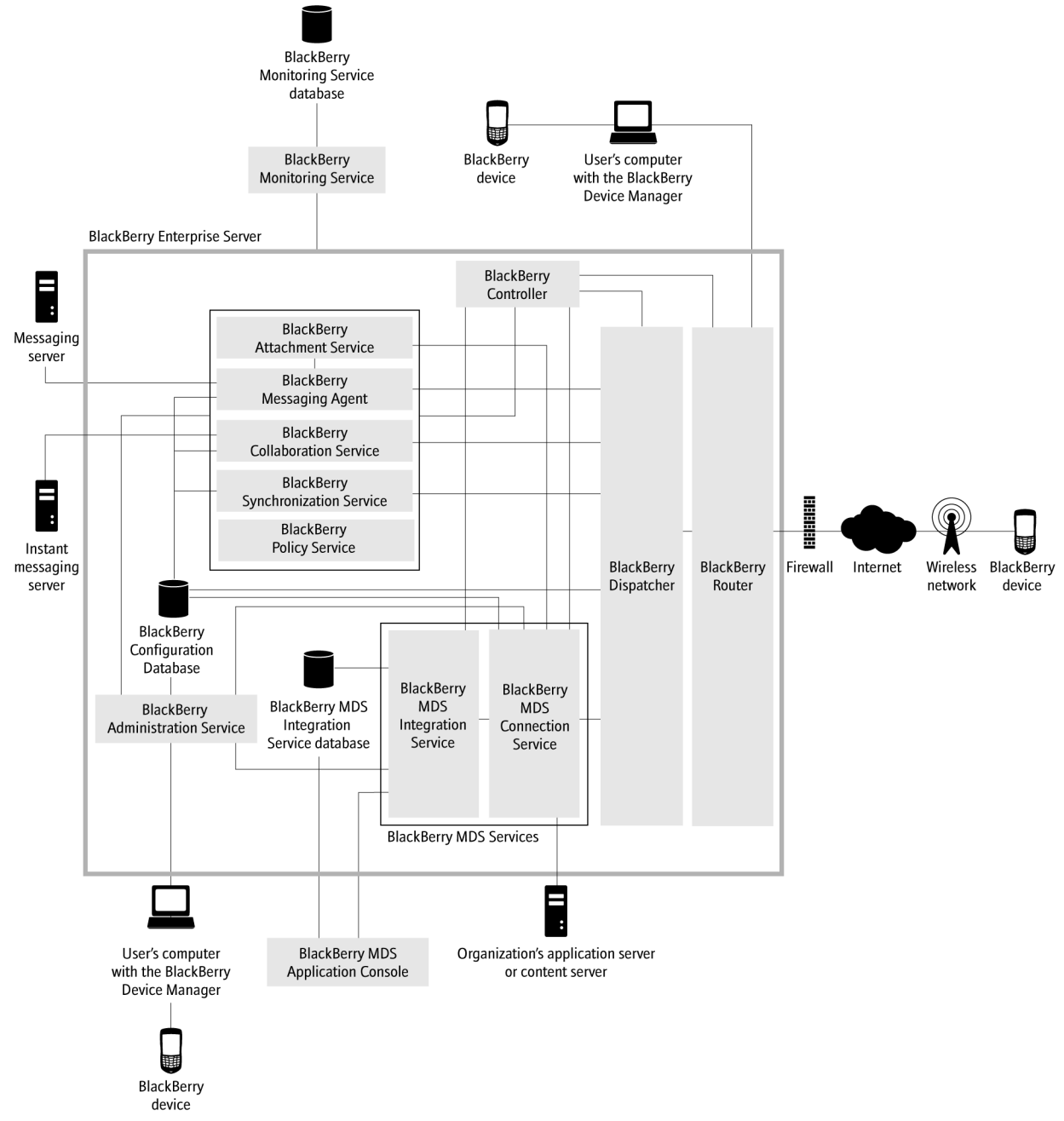
BlackBerry Enterprise Server architecture

2

Architecture: BlackBerry Enterprise Server

A BlackBerry® Enterprise Server consists of various components that are designed to perform the following actions:

- provide productivity tools and data from your organization's applications for your BlackBerry device users
- monitor other BlackBerry Enterprise Server components
- process, route, compress, and encrypt data
- communicate with the wireless network


BlackBerry Monitoring Service database
BlackBerry Monitoring Service
BlackBerry device
User's computer with the BlackBerry Device Manager
BlackBerry Enterprise Server
BlackBerry Controller
Messaging server
BlackBerry Attachment Service
BlackBerry Messaging Agent
BlackBerry Collaboration Service
BlackBerry Synchronization Service
BlackBerry Policy Service
Instant messaging server
BlackBerry Dispatcher
BlackBerry Router
Firewall
Internet
Wireless network
BlackBerry device
BlackBerry Configuration Database
BlackBerry Administration Service
BlackBerry MDS Integration Service database
BlackBerry MDS Integration Service
BlackBerry MDS Connection Service
BlackBerry MDS Services
User's computer with the BlackBerry Device Manager
BlackBerry MDS Application Console
Organization's application server or content server
BlackBerry device

Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service connects to the BlackBerry Configuration Database. You can use the BlackBerry Administration Service to manage the BlackBerry Domain, which includes BlackBerry Enterprise Server components, user accounts, and features for BlackBerry device administration.
BlackBerry Attachment Service	The BlackBerry Attachment Service converts supported message attachments to a format that users can view on their BlackBerry devices.
BlackBerry Collaboration Service	The BlackBerry Collaboration Service provides a connection between your organization's instant messaging server and the collaboration client on BlackBerry devices.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains configuration information that BlackBerry Enterprise Server components use. For example, the BlackBerry Configuration Database includes the following information: • details about the connection from a BlackBerry Enterprise Server to the wireless network • user list • address mappings between PINs and email addresses for BlackBerry MDS Connection Service push features
BlackBerry Controller	The BlackBerry Controller monitors BlackBerry Enterprise Server components and restarts them if they stop responding.
BlackBerry Dispatcher	The BlackBerry Dispatcher compresses and encrypts all data that BlackBerry devices send and receive. The BlackBerry Dispatcher sends the data through the BlackBerry Router, to and from the wireless network.
BlackBerry MDS Application Console	The BlackBerry MDS Application Console is a web-based administration console that you can use to manage BlackBerry MDS Runtime Applications and BlackBerry® Browser Applications that reside in the BlackBerry MDS Application Repository. You can use the BlackBerry MDS Application Console to send requests to a BlackBerry MDS Integration Service to install, update, and manage BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on BlackBerry devices.

Component	Description
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service permits users to access web content, the Internet, or your organization's intranet, and also permits applications on BlackBerry devices to connect to your organization's application servers or content servers for application data and updates.
BlackBerry MDS Integration Service	The BlackBerry MDS Integration Service provides application-level integration for BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on BlackBerry devices. You can use the BlackBerry MDS Integration Service to install BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on BlackBerry devices. The BlackBerry MDS Application Repository is a service hosted by the BlackBerry MDS Integration Service. The BlackBerry MDS Application Repository stores BlackBerry MDS Runtime Applications and BlackBerry Browser Applications. Your organization's developers can create and publish BlackBerry MDS Runtime Applications using the BlackBerry® MDS Studio or the BlackBerry® Plug-in for Microsoft® Visual Studio® developer tools. Your organization's developers can create BlackBerry Browser Applications using standard text editors and publish BlackBerry Browser Applications in the BlackBerry MDS Application Repository using the BlackBerry MDS Application Console.
BlackBerry Messaging Agent	The BlackBerry Messaging Agent connects to your organization's messaging server to provide messaging services, calendar management, address lookups, attachment viewing, attachment downloading, and encryption key generation. The BlackBerry Messaging Agent also acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes.
BlackBerry Monitoring Service	The BlackBerry Monitoring Service is a web-based application that is designed to help you monitor your organization's BlackBerry Domain. Administrators can use the BlackBerry Monitoring Service to troubleshoot issues and proactively monitor the health of your organization's BlackBerry Domain.
BlackBerry Monitoring Service database	The BlackBerry Monitoring Service database stores information that it collects about your organization's BlackBerry Enterprise Server environment in a Microsoft® SQL Server® database for 57 weeks. You can access the information from the database using standard SQL call operations.

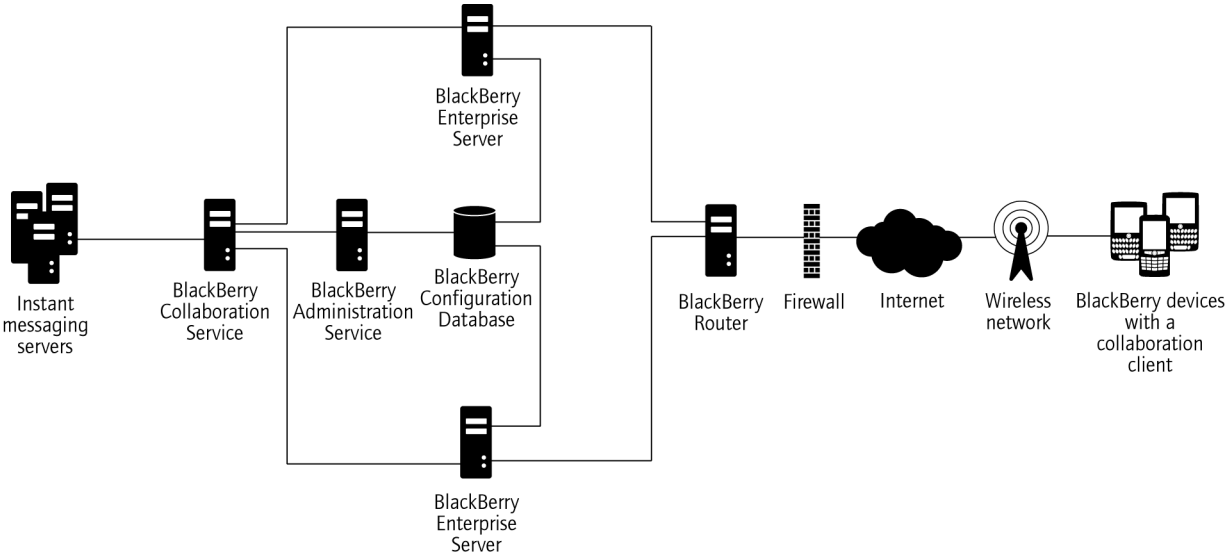
Component	Description
BlackBerry Policy Service	The BlackBerry Policy Service performs administration services over the wireless network. It sends IT policies and IT administration commands and provisions service books. IT policies and IT administration commands define BlackBerry device security, settings for synchronizing data over the wireless network, and other configuration settings on BlackBerry devices. The BlackBerry Policy Service also sends service books to configure settings for features and components on BlackBerry devices.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send data to and from BlackBerry devices. It also sends data over your organization's network to BlackBerry devices that are connected to computers that host the BlackBerry® Device Manager.
BlackBerry Synchronization Service	The BlackBerry Synchronization Service synchronizes organizer data between BlackBerry devices and the messaging server over the wireless network.
BlackBerry® Web Desktop Manager	The BlackBerry Web Desktop Manager is a web-based application that permits users to manage their BlackBerry devices. For example, users can activate BlackBerry devices, back up and restore data, select messaging options, synchronize data, and install applications. The BlackBerry Web Desktop Manager includes the BlackBerry Device Manager.
organization's application server or content server	Your organization's application server or content server provides push applications and intranet content that the BlackBerry MDS Services use.
instant messaging server	The instant messaging server stores instant messaging accounts.
messaging server	The messaging server stores email accounts.
user's computer with the BlackBerry Device Manager	The user's computer that hosts the BlackBerry Device Manager permits users to connect their BlackBerry devices to their computers using a serial or USB connection. The BlackBerry Enterprise Server and BlackBerry devices use the connection to send data between them. Data traffic from BlackBerry devices bypasses the wireless network when BlackBerry devices are connected to users' computers. The BlackBerry Device Manager connects to the BlackBerry Router, which sends data directly to BlackBerry devices. Users can install the BlackBerry Device Manager when they install the BlackBerry® Desktop Software or at another time. The BlackBerry Device Manager is an optional component, but it is required to support a bypass connection to the BlackBerry Router.

Architecture: Remote BlackBerry Collaboration Service

You can install the BlackBerry® Collaboration Service on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server. You can install the BlackBerry Collaboration Service on a remote computer to support multiple BlackBerry Enterprise Server instances, configure high availability for the BlackBerry Enterprise Server but exclude the BlackBerry Collaboration Service, or create a BlackBerry Collaboration Service pool that can support multiple BlackBerry Enterprise Server instances. For more information about configuring the BlackBerry Collaboration Service high availability, see the *BlackBerry Enterprise Server Planning Guide*.

The BlackBerry Collaboration Service uses a persistent socket connection for each instant messaging session. You can install the BlackBerry Collaboration Service on a remote computer to maximize the number of available sockets.

You can install only one type of BlackBerry Collaboration Service (for example, IBM® Lotus® Sametime®). Users can use only one type of collaboration client on their BlackBerry devices.



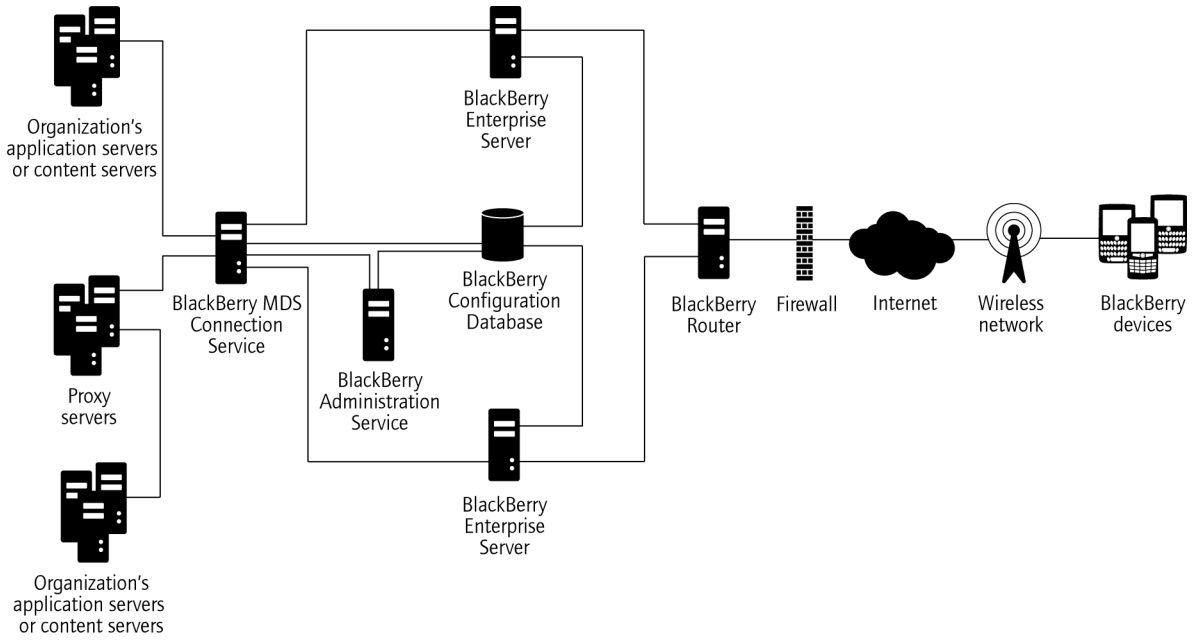
Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Collaboration Service and configure instant messaging features.
BlackBerry Collaboration Service	The BlackBerry Collaboration Service delivers messages between the instant messaging server, BlackBerry Enterprise Server, and BlackBerry devices.

Component	Description
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data that the BlackBerry Collaboration Service uses.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses instant messaging data that BlackBerry devices receive, and decompresses and decrypts instant messaging data that BlackBerry devices send.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send instant messaging data to and from BlackBerry devices.

Architecture: Remote BlackBerry MDS Connection Service

You can install the BlackBerry® MDS Connection Service on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server. The BlackBerry MDS Connection Service can use increased system resources when it processes requests for content. You can install the BlackBerry MDS Connection Service on a remote computer to minimize the impact on the delivery of messages and data, support multiple BlackBerry Enterprise Server instances, or create a BlackBerry MDS Connection Service pool that can support multiple BlackBerry Enterprise Server instances.

For information about configuring BlackBerry MDS Connection Service high availability, see the *BlackBerry Enterprise Server Planning Guide*.



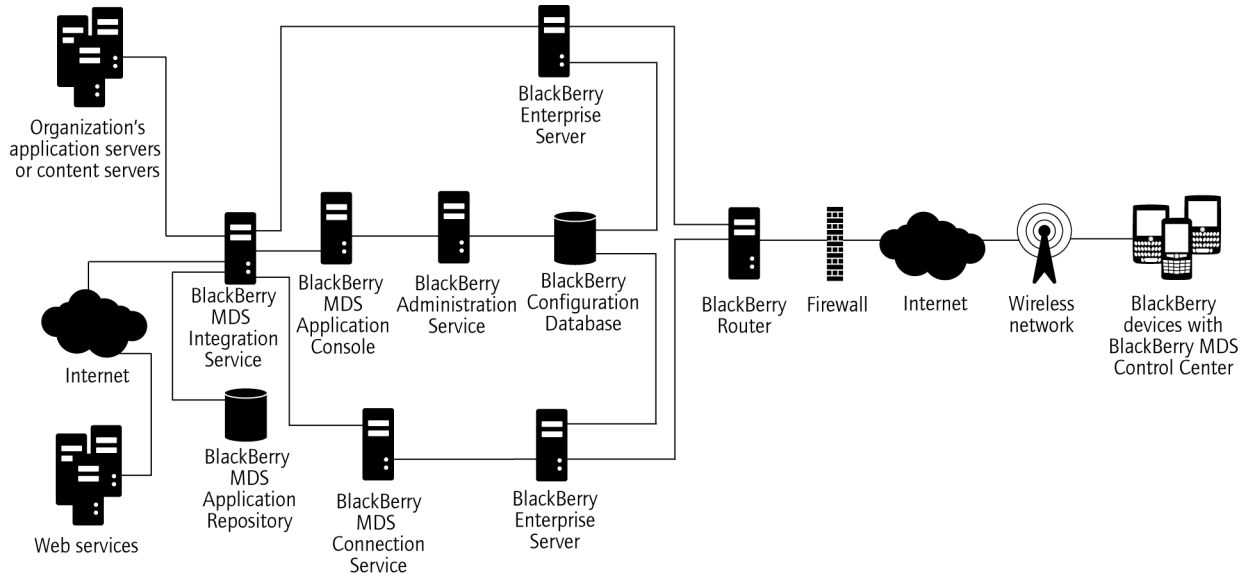
Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry MDS Connection Service, configure the central push server, and configure the browsing and application features.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains the configuration data that the BlackBerry MDS Connection Service uses.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses content data that BlackBerry devices receive, and decompresses and decrypts content data that BlackBerry devices send.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service processes requests for web content from the BlackBerry® Browser or a BlackBerry Java® Application, and it manages the connections between a BlackBerry® Application and the application that is located on your organization's application servers, web servers, or databases.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send content to and from BlackBerry devices.

Component	Description
organization's application servers or content servers	Your organization's application servers or content server provide push applications and intranet content for the BlackBerry MDS Services.
proxy servers	Proxy servers authenticate the BlackBerry Browser or a BlackBerry Java Application before they can access push applications or content data.

Architecture: Remote BlackBerry MDS Integration Service

You can install the BlackBerry® MDS Integration Service on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server however, the BlackBerry MDS Integration Service can use increased system resources when it processes requests for content. You can install the BlackBerry MDS Integration Service on a remote computer to minimize the impact on the delivery of messages and data to and from other BlackBerry Enterprise Server components and third-party applications, support multiple BlackBerry Enterprise Server instances, or create a remote BlackBerry MDS Integration Service pool for high availability.

For information about how to configure the BlackBerry MDS Integration Service for high availability, see the *BlackBerry Enterprise Server Planning Guide*.



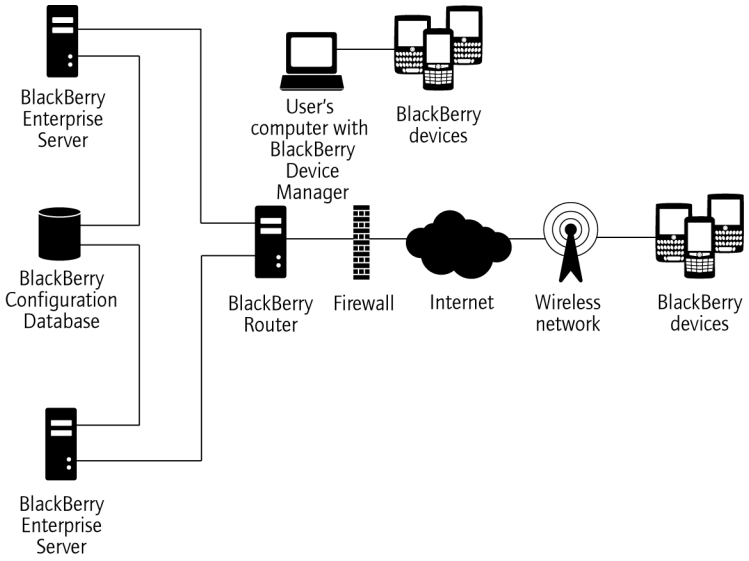
Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry MDS Integration Service, create software configurations, publish applications, and configure application features.
BlackBerry MDS Application Console	The BlackBerry MDS Application Console is a tool that manages applications published using the BlackBerry MDS Integration Service.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data for the BlackBerry MDS Integration Service.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses application data that BlackBerry devices receive, and decompresses and decrypts application data that BlackBerry devices send.
BlackBerry MDS Application Repository	The BlackBerry MDS Application Repository is a service that is hosted by the BlackBerry MDS Integration Service and stores the applications that your organization published so that users can install them on their BlackBerry devices.
BlackBerry MDS Integration Service	The BlackBerry MDS Integration Service permits a BlackBerry MDS Runtime Application to interact with server-side systems that expose standard interfaces or can be accessed by a direct database connection.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send application data to and from BlackBerry devices.
organization's application servers or content servers	Your organization's application servers or content servers provide push applications and intranet content used by the BlackBerry MDS Services.

Architecture: Remote BlackBerry Router

You can install the BlackBerry® Router on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server. You can install the BlackBerry Router on a remote computer if you want to support multiple BlackBerry Enterprise Server instances, create a remote BlackBerry Router pool, or if your organization's security policy requires that internal systems cannot make connections directly to the Internet and all systems must connect through another system in the DMZ.

The BlackBerry Router does not use many system resources, but it is a critical connection point for the BlackBerry® Enterprise Solution. You can install multiple BlackBerry Router instances for high availability if the primary BlackBerry Router becomes unavailable.

If you install the BlackBerry Router in the DMZ, you can permit users to log in to your organization's LAN remotely and you can deploy BlackBerry devices through a computer that is running the BlackBerry® Device Manager.



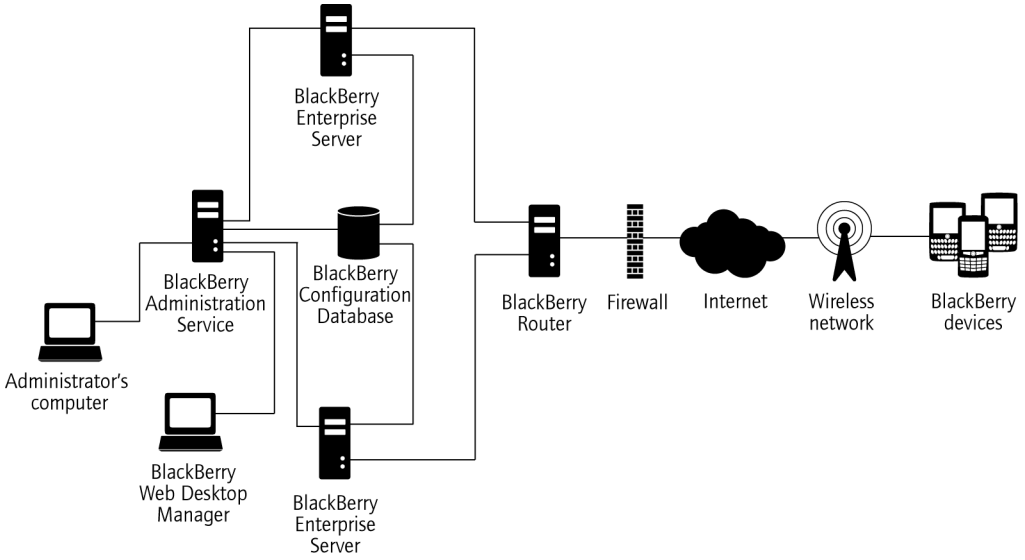
Component	Description
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data that the BlackBerry Administration Service manages.
BlackBerry Device Manager	The BlackBerry Device Manager permits BlackBerry devices to connect to the BlackBerry Router.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses data that BlackBerry devices receive, and decompresses and decrypts data that BlackBerry devices send.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send data to and from BlackBerry devices.

Architecture: Remote BlackBerry Administration Service

You can install the BlackBerry® Administration Service on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server. The BlackBerry Administration Service can use increased system resources when it processes requests. You can install the BlackBerry Administration Service remotely to minimize the impact on the delivery of messages and data, or to create a BlackBerry Administration Service pool to support multiple BlackBerry Enterprise Server instances.

For more information about configuring BlackBerry Administration Service high availability, see the *BlackBerry Enterprise Server Planning Guide*.

You can install the BlackBerry® Web Desktop Manager with the BlackBerry Administration Service. You can install the BlackBerry Web Desktop Manager separately to make sure that BlackBerry device users cannot access the computer that hosts the BlackBerry Enterprise Server.

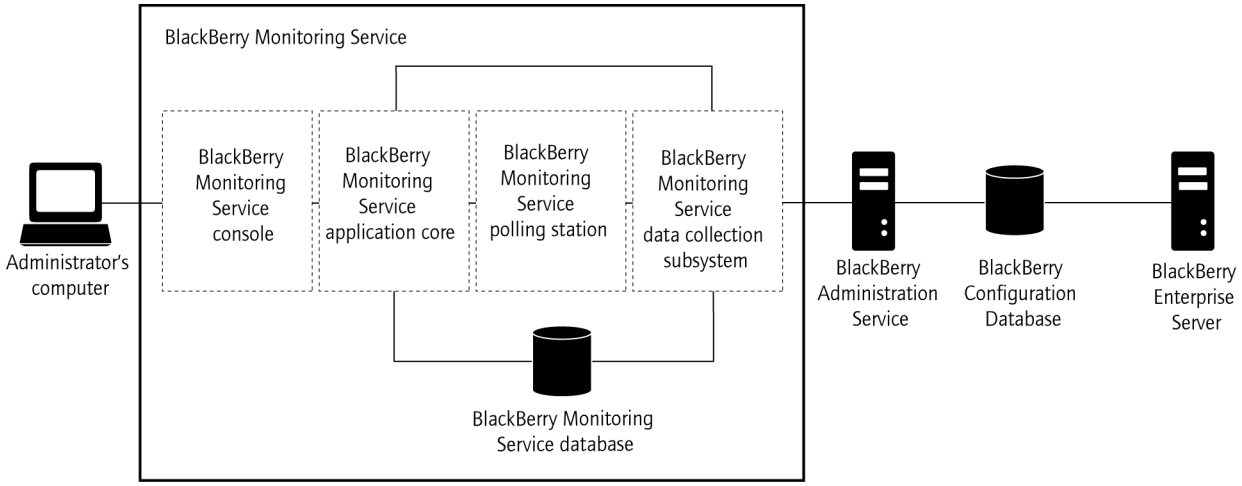


Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Enterprise Server, user accounts, and BlackBerry devices.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data that the BlackBerry Administration Service manages.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses data that BlackBerry devices receive, and decompresses and decrypts data that BlackBerry devices send.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send data to and from BlackBerry devices.
BlackBerry Web Desktop Manager	The BlackBerry Web Desktop Manager permits users to activate and manage their BlackBerry devices, back up and restore data, configure email settings, update the BlackBerry® Device Software, and install new applications.

Architecture: Remote BlackBerry Monitoring Service

You can install the BlackBerry® Monitoring Service on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server. If you install the BlackBerry Monitoring Service and BlackBerry Enterprise Server on the same computer, and that computer becomes unavailable, the BlackBerry Monitoring Service might not be able to monitor the BlackBerry Enterprise Server.

You can install the BlackBerry Monitoring Service database on the same computer as the BlackBerry Monitoring Service, on the same database server as the BlackBerry Configuration Database, or on another database server. You can install the BlackBerry Monitoring Service database on another database server if you do not want the BlackBerry Monitoring Service database to become unavailable at the same time as the BlackBerry Configuration Database, if your system resources are limited, or if you plan to run reports frequently.

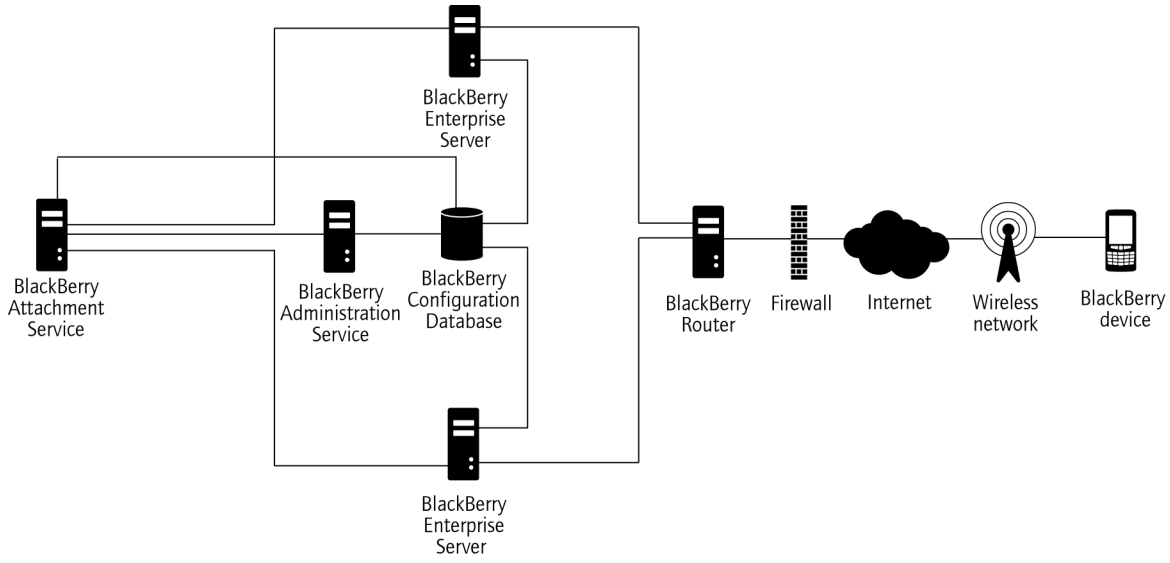


Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Enterprise Server, user accounts, and BlackBerry devices.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data that the BlackBerry Administration Service manages.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses the data that BlackBerry devices receive, and decompresses and decrypts the data that BlackBerry devices send.

Component	Description
BlackBerry Monitoring Service	The BlackBerry Monitoring Service is a web-based application that you can use to monitor your organization's BlackBerry Domain. The BlackBerry Monitoring Service consists of an administration console and Windows® services. The BlackBerry Monitoring Service console displays issues or events in the BlackBerry Domain that could cause an interruption to the BlackBerry Enterprise Server services and sends notification messages to contacts that you specify.
BlackBerry Monitoring Service console	The BlackBerry Monitoring Service console is a web-based application that provides a UI that you can use to manage and interact with the BlackBerry Monitoring Service.
BlackBerry Monitoring Service Application Core	The BlackBerry Monitoring Service Application Core processes rules that you define for monitoring your organization's BlackBerry Domain.
BlackBerry Monitoring Service Polling Engine	The BlackBerry Monitoring Service Polling Engine polls the BlackBerry Enterprise Server for SNMP data. The BlackBerry Monitoring Service Polling Engine sends the SNMP data to the BlackBerry Monitoring Service Application Core.
BlackBerry Monitoring Service database	The BlackBerry Monitoring Service database is a Microsoft® SQL Server® database where the BlackBerry Monitoring Service stores data that it collects about your organization's BlackBerry Domain for 57 weeks. You can access the data in the database using standard SQL call operations.
BlackBerry Monitoring Service Data Collection Subsystem	The BlackBerry Monitoring Service Data Collection Subsystem manages the persistence of historical monitoring data for building graphs. It also stores and retrieves data, and listens for data that the BlackBerry Monitoring Service Polling Engine sends.

Architecture: Remote BlackBerry Attachment Service

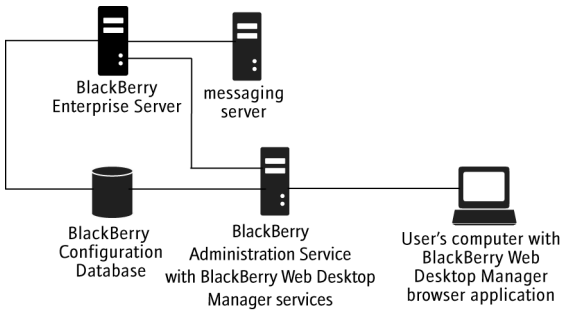
You can install the BlackBerry® Attachment Service on a computer that is separate from the computer that hosts the BlackBerry® Enterprise Server. You can install the BlackBerry Attachment Service remotely if you want to increase the number of conversion requests that can occur concurrently without impacting message delivery, support multiple BlackBerry Enterprise Server instances, or create a BlackBerry Attachment Service pool that can support multiple BlackBerry Enterprise Server instances. For more information about how to configure the BlackBerry Attachment Service for high availability, see the *BlackBerry Enterprise Server Planning Guide*.



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Attachment Service instances and set up attachment conversion features.
BlackBerry Attachment Service	The BlackBerry Attachment Service converts the attachment and returns the attachment data to the BlackBerry Attachment Connector.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains the conversion data that the BlackBerry Attachment Service uses when processing attachment data.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server receives requests to convert message attachments from BlackBerry devices and uses theBlackBerry Attachment Connector to send the attachment data to a BlackBerry Attachment Service instance for conversion. After the BlackBerry Attachment Service instance returns the converted attachment to the BlackBerry Attachment Connector, the BlackBerry Enterprise Server sends the attachment data to the user's BlackBerry device for viewing.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send email messages and attachments to and from BlackBerry devices.

Architecture: BlackBerry Web Desktop Manager

The BlackBerry® Web Desktop Manager consists of server-side services that are installed with the BlackBerry Administration Service and Microsoft® ActiveX® controls that are installed on the browser of the BlackBerry device user. HTTPS authentication secures the connection between the server and the browser.



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service is a web application that is a required component of the BlackBerry® Enterprise Server. Administrators use the BlackBerry Administration Service to manage user accounts; assign user groups, administrator roles, software configurations, and IT policies to user accounts; and manage servers and components in a BlackBerry Domain.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses data that BlackBerry devices receive, and decompresses and decrypts data that BlackBerry devices send.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains configuration information, such as BlackBerry Enterprise Server connection details and user information.
messaging server	The messaging server stores the email accounts of the BlackBerry device users.
user's computer with BlackBerry Web Desktop Manager browser application	The BlackBerry Web Desktop Manager browser application is the Microsoft ActiveX controls that a user installs in a browser to manage the BlackBerry device.
BlackBerry Administration Service and BlackBerry Web Desktop Manager services	The BlackBerry Administration Service and BlackBerry Web Desktop Manager services provide the server-side services for the BlackBerry Web Desktop Manager browser application.

BlackBerry Enterprise Server components and features 3

BlackBerry messaging and collaboration services

The BlackBerry® messaging and collaboration services provide a wireless extension of your organization's messaging environment. These services include the BlackBerry Messaging Agent, BlackBerry Collaboration Service, BlackBerry Synchronization Service, and BlackBerry Attachment Service.

BlackBerry Messaging Agent

The BlackBerry® Messaging Agent connects to your organization's messaging server and provides messaging services, calendar management, address lookups, attachment viewing, attachment downloading, and encryption key generation. The BlackBerry Messaging Agent acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes.

The BlackBerry Messaging Agent integrates with existing email accounts in your organization. The BlackBerry Messaging Agent redirects messages from users' email applications to their BlackBerry devices automatically. If users configure identical signatures on their BlackBerry devices and in their email accounts, recipients cannot distinguish between messages that users send from BlackBerry devices and messages that they send from email applications.

When users move or delete messages or mark messages as read or unread on their BlackBerry devices or in their email applications, the BlackBerry Messaging Agent reconciles changes over the wireless network between BlackBerry devices and email applications. By default, BlackBerry devices and the BlackBerry® Enterprise Server reconcile email messages over the wireless network.

Wireless messaging features

BlackBerry® device users can use many of the same messaging features that are available in the email applications on their computers.

Feature	Description
email reconciliation	The BlackBerry® Enterprise Server reconciles the status of messages between users' BlackBerry devices and their email applications. If users delete, archive, or move messages to personal folders in their email applications, the messages are deleted from the message list on the users' BlackBerry devices. If users mark messages as read or unread in their email applications, the messages appear with the same status on their BlackBerry devices.

Feature	Description
	You can turn off wireless email reconciliation.
email message filters	You or users can create and change email message filters. Email message filters determine the actions that the BlackBerry Enterprise Server takes if incoming messages match specific criteria: forward, forward with priority, or do not forward to BlackBerry devices. For example, users can create email message filters to forward messages from specific senders to their BlackBerry devices with high priority.
message forwarding	Users can turn off message forwarding to their BlackBerry devices (for example, if users are outside of a wireless coverage area). You can also turn off message forwarding to users' BlackBerry devices.
signature	Users can add a signature to all messages that they send from their BlackBerry devices. You can add a signature and disclaimers to all messages that the members of a user group send or a specific user sends.
out-of-office reply	Users can set and change their out-of-office replies using their BlackBerry devices.
contact lookup	Users can search for a contact's first name, last name, or both in their organization's directory. The BlackBerry Enterprise Server returns results for a maximum of 20 of the closest matches.
contact list updates	When users select contacts from the contact lookup results, they can add the contacts to the contact lists on their BlackBerry devices.
custom fields in the contact list	If your organization maintains custom fields in users' personal contact lists, you can map these fields to corresponding fields that appear in the contact list on BlackBerry devices. Users can use these custom fields to search for contacts on their BlackBerry devices.
attachments	Users can send messages that contain attachments from their BlackBerry devices. The BlackBerry Attachment Service does not convert these messages; the BlackBerry Messaging Agent processes them only. Attachments must meet the following requirements: • If a user sends one attachment in a message, the file size of the attachment cannot exceed 3 MB. • If a user sends multiple attachments in a message, the total file size of the attachments cannot exceed 5 MB. • If an attachment exceeds 64 KB, the BlackBerry device sends the attachment in multiple data packets.

Feature	Description
	Users can send messages with attachments only from supported BlackBerry devices that are running BlackBerry® Device Software version 4.2 or later. If you want to manage the system resources that the BlackBerry Messaging Agent uses to upload and send attachments, you can limit the file size of attachments or prevent users from attaching files to messages. For example, if too many users are sending large attachments, such as pictures or videos, you might want to limit the file size of supported attachments or turn off support for message attachments.
downloading attachments	Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can download attachments and store them on their BlackBerry devices. Users can open and make changes to the downloaded attachments using an appropriate third-party application on their BlackBerry devices. Users can open supported attachment file formats using the media application on their BlackBerry devices. To manage network resources in your organization's environment, you can change the maximum file size of attachments that users can download to their BlackBerry devices.
save sent messages	Users can configure their BlackBerry devices to save copies of messages that they send from their BlackBerry devices in the sent items folder in their email applications.
personal distribution lists	Users with BlackBerry Device Software version 5.0 or later can view personal distribution lists in their contact lists. Users can send messages to the personal distribution lists and delete personal distribution lists from their BlackBerry devices.
public folders	Users with BlackBerry Device Software version 5.0 or later can view and use contacts in public folders from their BlackBerry devices, and copy the contacts to their contact lists. Users can only view the public folders that they have the appropriate permissions for. Users can specify which public folders they want to synchronize to their BlackBerry devices using the BlackBerry® Desktop Manager or BlackBerry® Web Desktop Manager. You can limit the number of public folders that users can synchronize to their BlackBerry devices.
personal folders	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can add, delete, move, and rename personal folders from their BlackBerry devices.

Feature	Description
follow up flag	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can flag messages from their BlackBerry devices and set reminder times.
personal contact subfolders	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can view personal contact subfolders on their BlackBerry devices and change contact information. Users can specify which contact subfolders that they want to synchronize to their BlackBerry devices using BlackBerry Desktop Manager or BlackBerry Web Desktop Manager. You can limit the number of contact subfolders that a user can synchronize to their BlackBerry devices.
forwarding calendar entries	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can forward meeting invitations and calendar entries from their BlackBerry devices.
availability of meeting invitees	Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can view the availability of meeting invitees on their BlackBerry devices. You can turn off this feature using the BlackBerry Administration Service.
remote search for email messages	Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can search for email messages that are located on the messaging server from their BlackBerry devices. You can turn off this feature using the BlackBerry Administration Service.
rich content email messages	Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can view HTML and rich content email messages. You can turn off this feature using the BlackBerry Administration Service.

Access to documents on a network from BlackBerry devices

Users with BlackBerry® devices that are running BlackBerry® Device Software version 5.0 or later can use a file browser on their BlackBerry devices to access documents that are located in a shared location such as a network drive. Users can view document information such as the file name, file type, file size, author, and date the file was last changed. Users must have access to the shared location using their network credentials, or you must configure the BlackBerry® Enterprise Server to access the documents for the users.

Users can send the documents as attachments in messages or instant messages, view supported document types using the attachment viewer, download copies of the documents, or open and make changes to the documents using an appropriate third-party application on their BlackBerry devices. They can also add attachments from messages or documents that they access using the BlackBerry® Browser to the network drive.

BlackBerry Collaboration Service

The BlackBerry® Collaboration Service provides a connection between your organization's instant messaging server and the collaboration client on BlackBerry devices. The BlackBerry Collaboration Service integrates with existing instant messaging applications. The BlackBerry® Enterprise Server supports the following collaboration clients:

- BlackBerry® Client for use with Microsoft® Office Live Communications Server 2005
- BlackBerry® Client for use with Microsoft® Office Communications Server 2007
- BlackBerry® Client for IBM® Lotus® Sametime®
- BlackBerry® Client for Novell® GroupWise® Messenger

The BlackBerry Collaboration Service sends messages between your organization's instant messaging server, BlackBerry Enterprise Server, and BlackBerry devices using public APIs, a Research In Motion proprietary protocol, and protocols that are defined by IBM, Microsoft, and Novell.

Instant messaging features

Using the collaboration clients on their BlackBerry® devices, users can use many of the same features that are available in the instant messaging applications on their computers.

Feature	Description
session management	You can specify the number of simultaneous instant messaging sessions that the BlackBerry Collaboration Service supports. You can also specify a timeout threshold, after which the BlackBerry Collaboration Service ends inactive sessions automatically and permits new sessions to start. You can control whether users of specific versions of the BlackBerry® Client for IBM® Lotus® Sametime® or the BlackBerry® Client for Novell® GroupWise® Messenger can see an icon on their BlackBerry devices when contacts in their contact lists are using the same collaboration clients. By default, the icon appears.
conversations with multiple contacts	Users can start and manage conversations with multiple instant messaging contacts on their BlackBerry devices.
availability status	Users can change their availability status when they are logged in to their collaboration clients. For example, users can set their availability status to away or busy.
presence updates	Using the latest versions of the collaboration clients, users can set their availability status to display as away if they do not use their BlackBerry devices for a specified period of time.

Feature	Description
access levels	Using the latest version of the BlackBerry® Client for use with Microsoft® Office Communications Server 2007, users can set the access level of contacts in their contact lists. Each access level consists of rules that define how contacts can interact with a user through the instant messaging application. For example, users can assign the Personal access level to their contacts.
contact pictures	Using the latest versions of the collaboration clients, users can add pictures to the contacts in their contact lists. The pictures that users add using the collaboration clients on their BlackBerry devices are not synchronized with the instant messaging applications on users' computers.
synchronized contact lists	The instant messaging contact lists on users' BlackBerry devices are synchronized with the contact lists in their organization's instant messaging application.
contact alerts	Users can request alerts when specific contacts become available.
file transfer	Using the latest version of the BlackBerry Client for IBM Lotus Sametime, users can send files to contacts in their contact lists. Recipients can open supported file formats on their BlackBerry devices.
link instant messaging contacts to the contact list on BlackBerry devices	Using the latest versions of the collaboration clients, users can link instant messaging contacts to existing contact list entries on their BlackBerry devices. They can also create new contact list entries for instant messaging contacts and populate them with information from their organization's messaging server.
send email messages from contact list	Using the latest versions of the collaboration clients, users can send email messages to contacts directly from their contact lists.
call contacts	Using the latest versions of the collaboration clients, users can call instant messaging contacts directly from their contact lists. After a user starts an instant messaging conversation with a contact, the user can make a call to that contact from the conversation window. Phone numbers for contacts are retrieved from the messaging server or from the contact list on the BlackBerry device if the user is linked to an existing contact list entry.
email conversation history	Using the latest versions of the collaboration clients, users who participate in an instant messaging conversation can send the history of the conversation as an email message to other participants of the conversation and to additional contacts from their contact lists on their BlackBerry devices.
embedded links	Users can click phone numbers in instant messages to make calls. They can also click links in instant messages to view web pages.

Feature	Description
public groups	Using the latest version of the BlackBerry Client for IBM Lotus Sametime, users can add public groups to their instant messaging contact lists.
location information	Using the latest version of the BlackBerry Client for IBM Lotus Sametime or the BlackBerry Client for use with Microsoft Office Communications Server 2007, users can set their current location to display in their contact information. For example, users can set their current location to In the office. This feature is not available if your organization's environment uses IBM Lotus Sametime version 6.5.1.
announcements	Using the latest version of the BlackBerry Client for IBM Lotus Sametime or BlackBerry Client for Novell GroupWise Messenger, users can send announcements to groups or multiple contacts in their contact lists.
send messages to contacts who are not included in a contact list	Using the latest version of the BlackBerry Client for IBM Lotus Sametime, BlackBerry® Client for use with Microsoft® Office Live Communications Server 2005, or BlackBerry Client for use with Microsoft Office Communications Server 2007, users can send instant messages to contacts that are not included in their contact lists.
dormant mode	The collaboration clients enter dormant mode after five minutes of inactivity. In dormant mode, the applications do not receive presence updates for contacts. Dormant mode is designed to reduce wireless network traffic in an organization's messaging environment. The collaboration clients turn off dormant mode when users open or use the applications, or receive conference requests, alerts, or messages from contacts.

BlackBerry Synchronization Service

The BlackBerry® Synchronization Service synchronizes organizer data such as tasks, memos, and contacts over the wireless network so that the entries on BlackBerry devices are consistent with the entries in the email applications. With wireless data synchronization and wireless email reconciliation, users are not required to connect their BlackBerry devices to the BlackBerry® Desktop Software to synchronize organizer data and reconcile email messages.

The BlackBerry Synchronization Service backs up user settings and data over the wireless network from BlackBerry devices to the BlackBerry Configuration Database. You can restore the user settings and data to BlackBerry devices when the BlackBerry devices are activated over the wireless network. By default, the BlackBerry® Enterprise Server automatically backs up the user settings and data over the wireless network.

Synchronization features

You can change the settings for synchronization features so that users can manage the user experience and system resources in your organization's environment.

Feature	Description
initial synchronization	When the BlackBerry® Enterprise Server sends service books to BlackBerry devices to turn on wireless data synchronization, an initial data synchronization process starts. The process synchronizes the data for calendar items and messages between users' BlackBerry devices and the email applications on their computers. It also resolves conflicting or duplicate entries to prevent data loss. By default, the calendar on the BlackBerry device synchronizes up to 31 days in the past from the activation date, and up to 28 years into the future from the activation date.
synchronization settings	You can configure settings for wireless data synchronization that apply to specific users, user groups, or all users on all BlackBerry Enterprise Server instances. You can define which organizer data items the BlackBerry Synchronization Service synchronizes, how data conflicts are resolved, and whether changes are synchronized in both directions or in one direction only between BlackBerry devices and email applications. You can use IT policies to configure the settings for wireless data synchronization.
support for different types of user access	The BlackBerry Enterprise Server requires access to the organizer application databases for all users. You can define the location of the database replicas in each user's profile, create roaming user profiles, or use web access templates in your organization's messaging environment.
synchronization of contact pictures	The BlackBerry Synchronization Service synchronizes contact pictures between users' BlackBerry devices and the email applications on their computers. If users use their BlackBerry devices to add, change, or delete contact pictures, the contact lists in their email applications reflect the changes. The BlackBerry Synchronization Service cannot synchronize contact pictures that exceed 32 KB.

BlackBerry Attachment Service

The BlackBerry® Attachment Service converts supported message attachments into a format that users can view on their BlackBerry devices. The BlackBerry Attachment Service processes attachments and converts them into a binary format that retains most of the layout, appearance, and navigation of the original attachments. You do not have to install the applications that are associated with the attachment formats on BlackBerry devices. The attachment viewer installs automatically with the BlackBerry® Device Software.

The BlackBerry Attachment Service receives attachments that are embedded in messages from the messaging server, through the BlackBerry Messaging Agent. The BlackBerry Attachment Service also receives attachments that are accessed through links in the BlackBerry® Browser.

The BlackBerry Attachment Service enables users to play supported audio attachments on supported BlackBerry devices that are running BlackBerry Device Software version 4.2 or later. The BlackBerry Attachment Service can convert .wav files into an audio format that a BlackBerry device series supports (for example, .mp3 files on BlackBerry® 8700 Series devices).

Attachment file formats that the BlackBerry Attachment Service supports

Format	Extension
Adobe® Acrobat® versions 1.1, 1.2, 1.3, and 1.4	.pdf
ASCII text	.txt
audio	.amr, .mp3, .wav, .wma
Corel® WordPerfect® versions 6.0, 7.0, 8.0, 9.0 (2000), and 10.0	.wpd
HTML	.htm, .html
images	.bmp, .gif, .jpeg, .jpg, .png, .tif, .tiff, .wmf
Microsoft® Excel® versions 97, 2000, 2003, 2007, and XP	.xls, .xlsx
Microsoft® PowerPoint® versions 97, 2000, 2003, 2007, and XP	.pps, .ppt, .pptx
Microsoft® Word versions 97, 2000, 2003, 2007, and XP	.doc, .dot, .docx
OpenDocument	.odt
RTF	.rtf
ZIP archives	.zip

BlackBerry MDS

The BlackBerry® Mobile Data System is a flexible framework for application development that you can use to add and manage applications in your organization's environment. As a component of the BlackBerry® Enterprise Server, the BlackBerry MDS offers security, wireless connectivity, and manageability options. It also supports several preferred development methods that you can use to create wireless applications and deliver them to BlackBerry devices. To simplify the integration of wireless applications with existing applications and systems, the BlackBerry MDS uses standards-based methods and protocols.

Component	Description
BlackBerry MDS Services	You can use the BlackBerry MDS Services to send wireless applications to BlackBerry devices, and to maintain and manage wireless applications on BlackBerry devices. The BlackBerry MDS Services are designed to provide wireless connectivity between applications on BlackBerry devices and your organization's existing applications. The BlackBerry MDS Services include the following components: • **BlackBerry MDS Integration Service**: The BlackBerry MDS Integration Service enables BlackBerry MDS Runtime Applications to interact with back-end systems using web services or direct database connections. You can install the BlackBerry MDS Integration Service when you install the BlackBerry Enterprise Server. • **BlackBerry MDS Connection Service**: The BlackBerry MDS Connection Service processes requests for web content from the BlackBerry® Browser or from BlackBerry Java® Applications. The BlackBerry MDS Connection Service also manages TCP/IP and HTTP connections between BlackBerry Applications and the applications that reside on your organization's application servers, web servers, or databases that are located inside your organization's firewall.
BlackBerry MDS development tools	Developers in your organization can use development tools to create the following types of wireless applications for BlackBerry devices: BlackBerry Browser Applications, BlackBerry Java Applications, and BlackBerry MDS Runtime Applications. For more information about BlackBerry MDS development tools, visit www.blackberry.com/developers.
BlackBerry MDS device software	BlackBerry devices use the following BlackBerry MDS device software to run BlackBerry Applications:

Component	Description
	• BlackBerry® MDS Runtime: runs BlackBerry MDS Runtime Applications • BlackBerry APIs and Java® ME: runs BlackBerry Java Applications; standard on BlackBerry devices • BlackBerry Browser: runs BlackBerry Browser Applications and is standard on BlackBerry devices To download the BlackBerry MDS Runtime, visit www.blackberry.com.

For more information about the BlackBerry MDS and the types of BlackBerry Applications, visit www.blackberry.com/developers to see the *BlackBerry Mobile Data System Technical Overview*.

BlackBerry Applications

BlackBerry® devices support BlackBerry® Browser Applications, BlackBerry Java® Applications, and BlackBerry® MDS Runtime Applications. Application developers in your organization can create BlackBerry Applications using BlackBerry development tools or third-party development tools. You can install and manage BlackBerry Java Applications on BlackBerry devices using the BlackBerry Administration Service. You can install and manage BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on BlackBerry devices using the BlackBerry MDS Application Console.

For more information about the options for developing BlackBerry Applications, visit www.blackberry.com/developers to see the *BlackBerry Mobile Data System Technical Overview*.

BlackBerry Java Applications

BlackBerry® Java® Applications can range from simple applications, such as a game on BlackBerry devices, to complex applications with advanced UIs and various options for data management, storage, and network communication. BlackBerry Java Applications can use a client-only architecture (that is, the applications do not send data to or receive data from a content server) or they can use a client/server application model (that is, the applications send data to and receive data from a content server). For example, a developer can create a BlackBerry Java Application so that users can send data to and receive data from a central sales database.

Developers can create BlackBerry Java Applications using the BlackBerry® Java® Development Environment, the BlackBerry® JDE Plug-in for Eclipse®, or other Java authoring tools. BlackBerry devices run BlackBerry Java Applications using BlackBerry APIs and Java ME, which are standard on BlackBerry devices.

For more information about developing and customizing BlackBerry Applications, visit www.blackberry.com/developers.

BlackBerry MDS Runtime Applications

BlackBerry® MDS Runtime Applications are lightweight, rich-client applications that are created using BlackBerry® MDS Studio or the BlackBerry® Plug-in for Microsoft® Visual Studio®. BlackBerry MDS Runtime Applications communicate with an organization's systems through the BlackBerry MDS Integration Service, a component of the BlackBerry® Enterprise Server. BlackBerry MDS Runtime Applications can range from simple to complex, but they are typically forms-based applications that users can use to access web services or databases that are located inside your organization's firewall. Web services or a database contain the data and operations that developers can use to create BlackBerry MDS Runtime Applications. Web services or a database also process the data that they receive from BlackBerry MDS Runtime Applications. For example, a developer can create a BlackBerry MDS Runtime Application so that users can look up data from a directory in your organization.

Using the latest versions of the BlackBerry MDS Studio Plug-in for Eclipse or the BlackBerry Plug-in for Microsoft Visual Studio, application developers in your organization can create BlackBerry MDS Runtime Applications that standard applications on BlackBerry devices (for example, the contact list) and custom BlackBerry Java® Applications can invoke. Developers can also create BlackBerry MDS Runtime Applications that can invoke standard applications on BlackBerry devices, custom BlackBerry Java Applications, or other BlackBerry MDS Runtime Applications.

You must install and activate the BlackBerry MDS Runtime on BlackBerry devices before you install BlackBerry MDS Runtime Applications on BlackBerry devices.

For more information about developing and customizing BlackBerry Applications, visit www.blackberry.com/developers.

BlackBerry Browser Applications

BlackBerry® Browser Applications are simplified, web-based applications that you can use to push web content to the BlackBerry Browser on BlackBerry devices. Developers can create BlackBerry Browser Applications using BlackBerry templates or standard web development tools.

The BlackBerry MDS Integration Service includes a Browser Push Engine that can poll specific web addresses for changes or updates, and push the web content to BlackBerry devices at an interval that developers specify. For example, a developer can create a BlackBerry Browser Application that pushes a web page about the local weather to BlackBerry devices every morning.

The BlackBerry® Enterprise Server supports the following types of BlackBerry Browser Applications.

Type	Description
browser channel push applications	An icon displays on the Home screens of users' BlackBerry devices to indicate whether users viewed the latest version of the web content that the Browser Push Engine has pushed to their BlackBerry devices.
browser cache push applications	The Browser Push Engine pushes web content to the cache of the BlackBerry Browser on users' BlackBerry devices. To view the web content, users browse to the appropriate web address using the BlackBerry Browser.

Type	Description
browser message push applications	A message appears in the message list on users' BlackBerry devices to provide a link to new or updated web content.

For more information about developing and customizing BlackBerry Applications, visit www.blackberry.com/developers.

BlackBerry MDS Connection Service

The BlackBerry® MDS Connection Service connects wireless applications on BlackBerry devices to the applications on an organization's application servers or web servers. After a wireless application is installed on BlackBerry devices, the application can receive data from push applications that are located on application servers or web servers. The application can also receive data by sending pull requests from BlackBerry devices to applications that are located on application servers or web servers. The BlackBerry MDS Connection Service processes push and pull requests and delivers data and updates to BlackBerry Applications.

The BlackBerry MDS Connection Service also receives and responds to web requests from the BlackBerry® Browser and other BlackBerry Applications, so that users can view Internet and intranet content on their BlackBerry devices. The BlackBerry MDS Connection Service sends login requests and requests for instant messaging sessions from BlackBerry devices to the BlackBerry Collaboration Service. If you stop the BlackBerry MDS Connection Service, you also stop the BlackBerry Collaboration Service.

Feature	Description
protocol connections	You can define connections to the web servers on your organization's intranet or the Internet using standard Internet protocols such as HTTP, HTTPS, and TCP/IP.
encrypted communications	The BlackBerry MDS Connection Service encrypts content using the same standard BlackBerry encryption that the BlackBerry Dispatcher uses to encrypt messages and other data.
data conversion	The BlackBerry MDS Connection Service converts data from application servers and web servers to a format that BlackBerry Applications can interpret and display.
data optimization	The BlackBerry MDS Connection Service processes content that users can view in the BlackBerry Browser. For example, the BlackBerry MDS Connection Service can change the data format or remove extraneous data to reduce network traffic.
authentication methods	You can configure authentication requirements that match your organization's sign-on scheme using standard methods such as NTLM, Kerberos™, and LTPA. You can also define a period of time after which the BlackBerry MDS Connection Service requests user information and caches cookies.

Feature	Description
	You can use two-factor authentication to create VPN connections between wireless applications on BlackBerry devices and your organization's application servers and web servers.
integration with proxy servers	You can provide access to specific content through your organization's proxy servers using the following items: • proxy exclusion list, which defines the organization-specific URLs that the BlackBerry MDS Connection Service uses to connect directly to external web services instead of routing the connections through your organization's proxy server • proxy auto-configuration (.pac) file
access control	You can configure push initiators and push rules that define which server-side push applications can send application data and updates to BlackBerry devices, and which users can receive push requests. You can configure pull rules to specify which web servers users can access using the BlackBerry Browser and other applications on BlackBerry devices.
media content management	You can control which media files users can receive and access using the BlackBerry Browser and BlackBerry Applications. You can prevent users from receiving specific media types (for example, video files) or specific subtypes of media (for example, .mp3 files). You can also configure size limits for media files that users can receive on their BlackBerry devices.

BlackBerry MDS Integration Service

The BlackBerry® MDS Integration Service permits you to install, update, and manage BlackBerry MDS Runtime Applications on BlackBerry devices. The BlackBerry MDS Integration Service supports standard methods of integrating wireless applications and enterprise applications, for example, by permitting BlackBerry MDS Runtime Applications to access and use web services on an application server.

Your organization's developers can create BlackBerry MDS Runtime Applications using the BlackBerry® MDS Studio or BlackBerry® Plug-in for Microsoft® Visual Studio®, and publish the applications to the BlackBerry MDS Application Repository. You can install, update, and remove BlackBerry MDS Runtime Applications on BlackBerry devices over the wireless network, and you can manage different versions of BlackBerry MDS Runtime Applications.

Feature	Description
installation options	You can prevent users from searching for BlackBerry MDS Runtime Applications. You can also require users to install, update, or remove specific BlackBerry MDS Runtime Applications from BlackBerry devices.
encrypted communication	The BlackBerry MDS Integration Service encrypts all data that it sends to and receives from BlackBerry devices.
troubleshooting tools	A series of error messages display when unexpected behavior occurs, such as if an application cannot connect to a content server.
message monitoring	BlackBerry MDS Runtime Applications can request data from application servers or web servers using a series of messages. Web servers return the requested data using the same message format. You can monitor the messages that BlackBerry MDS Runtime Applications send to or from the application servers or web servers that host application content.
PKI-compliant application certificates	The BlackBerry MDS Studio creates certificates and uses them to sign applications that comply with the PKI X.509 standard. You can use certificates to encrypt the connections that the BlackBerry MDS Integration Service establishes to sensitive content.
control user access and permissions	You can configure IT policy rules in the BlackBerry MDS Integration Service policy group to control how users can search for and access BlackBerry MDS Runtime Applications, and to define whether BlackBerry MDS Runtime Applications can access data from other applications on BlackBerry devices.
performance management	You can specify message queue limits for data that BlackBerry MDS Runtime Applications send and receive.

Managing BlackBerry Java Applications and BlackBerry Device Software

You can use the BlackBerry® Administration Service to install and manage the BlackBerry® Device Software and BlackBerry Java® Applications on BlackBerry devices.

To send BlackBerry Java Applications to BlackBerry devices, you must first add the applications to the application repository. You can use the application repository to store and manage all versions of the BlackBerry Java Applications that you want to install on, update on, or remove from BlackBerry devices.

In the BlackBerry Administration Service, you create software configurations to specify the versions of the BlackBerry Device Software and BlackBerry Java Applications that you want to install on, update on, or remove from BlackBerry devices. You also use software configurations to specify which applications are required, optional, or not permitted on BlackBerry devices. When you create a software configuration, you must also specify whether users can install applications that are not listed in the software configuration on their BlackBerry devices.

When you add a BlackBerry Java Application to a software configuration, you must assign an application control policy to the application to specify what resources the application can access on BlackBerry devices. You can use default application control policies or you can create and use custom application control policies for the application. If you permit users to install unlisted applications, you must create an application control policy for unlisted applications that specifies what resources the applications can access on BlackBerry devices.

When you assign a software configuration to a group or individual user accounts, the BlackBerry Administration Service creates a deployment job to install the BlackBerry Device Software and BlackBerry Java Applications on BlackBerry devices and to apply access control policies to BlackBerry devices. A deployment job consists of a number of tasks. Each task manages the delivery of a specific object (for example, a BlackBerry Java Application or an access control policy) to a BlackBerry device by communicating with the appropriate BlackBerry® Enterprise Server components.

If you assign more than one software configuration to a user account, all of the settings in the multiple software configurations are applied to the user's BlackBerry device. The BlackBerry Enterprise Server resolves conflicting settings using predefined reconciliation rules and prioritized rankings that you can specify using the BlackBerry Administration Service. After you install the BlackBerry Device Software and BlackBerry Java Applications on BlackBerry devices, you can view details about how the BlackBerry Administration Service resolved software configuration conflicts.

For more information about installing and managing the BlackBerry Device Software on BlackBerry devices, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Device Software Update Guide*.

BlackBerry MDS Application Console

The BlackBerry® MDS Application Console is a web-based administration console that you can use to manage BlackBerry® MDS Runtime Applications and BlackBerry® Browser Applications that are located in the BlackBerry MDS Application Repository. You can use the BlackBerry MDS Application Console to send requests to a BlackBerry MDS Integration Service to install or update BlackBerry MDS Runtime Applications and BlackBerry Browser Applications on BlackBerry devices, or remove the applications from BlackBerry devices. You must use the BlackBerry Administration Service to manage BlackBerry Java® Applications on BlackBerry devices. You install the BlackBerry MDS Application Console when you install the BlackBerry MDS Integration Service.

The BlackBerry MDS Application Console supports BlackBerry MDS Integration Service version 5.0 or later only.

BlackBerry device management

You can use the BlackBerry® Enterprise Server to control how you implement, maintain, and upgrade BlackBerry devices across your organization.

Controlling third-party applications on BlackBerry devices

Feature	Description
control the installation and removal of third-party applications	You can use the BlackBerry® Administration Service to install applications on BlackBerry devices over the wireless network, or you can permit users to download and install third-party applications on their BlackBerry devices. You can remove applications from BlackBerry devices over the wireless network, and you can also prevent users from downloading applications.
control the resources that third-party applications can access	You can use standard application control policies or create custom application control policies to specify the resources that third-party applications can access on BlackBerry devices (for example, message, phone, and key store). You can create IT policies that specify the types of connections that third-party applications on BlackBerry devices can establish (for example, opening network connections inside the firewall).
control the availability of BlackBerry® MDS Runtime Applications	Use BlackBerry MDS Integration Service IT policy rules to control whether users can search for and install BlackBerry MDS Runtime Applications in the BlackBerry MDS Application Repository.

BlackBerry Enterprise Solution security

The BlackBerry® Enterprise Solution is designed to encrypt data in transit at all points between BlackBerry devices and the BlackBerry® Enterprise Server to help protect your organization from data loss or alteration. Only the BlackBerry Enterprise Server and a BlackBerry device can decrypt the data that they send between each other. If events that threaten the wireless security of your organization occur, the BlackBerry Enterprise Server is designed to prevent third parties, including wireless service providers, from accessing your organization's potentially sensitive information in a decrypted format.

The BlackBerry Enterprise Solution uses symmetric key cryptography to encrypt messages and user data that it sends over the transport layer. Symmetric key cryptography provides the following criteria for the security of wired and wireless solutions.

Criteria	Description
confidentiality	The BlackBerry Enterprise Solution uses encryption to help ensure that only the intended message recipients can view the contents of the messages.

Criteria	Description
integrity	The BlackBerry Enterprise Solution helps protect each message that a BlackBerry device sends using one or more message keys. Designed to prevent a third party from decrypting or altering the message data, the message keys consist of random data. The BlackBerry Enterprise Solution is designed so that only the BlackBerry Enterprise Server and a BlackBerry device know the value of a master encryption key, recognize the format of a decrypted and decompressed message, and automatically reject a message that is not encrypted with the correct master encryption key.
authenticity	A BlackBerry device authenticates itself with the BlackBerry Enterprise Server to prove that it knows the master encryption key before the BlackBerry Enterprise Server can send data to the BlackBerry device.

Master encryption keys

The BlackBerry® Enterprise Server and the BlackBerry device each store a copy of the unique master encryption key of the BlackBerry device.

When you activate a BlackBerry device over the wireless network, the BlackBerry Enterprise Server and BlackBerry device use an authenticated link to communicate the value of the master encryption key.

For a user to send and receive messages on the BlackBerry device, the BlackBerry Enterprise Server and BlackBerry device must store matching copies of the master encryption key of the BlackBerry device. If the stored keys do not match, the following actions occur:

- BlackBerry Enterprise Server and BlackBerry device delete messages that they receive from each other because they cannot decrypt them
- BlackBerry device requires the user to generate a new master encryption key

Standard BlackBerry encryption

The BlackBerry® Enterprise Solution uses a symmetric key encryption algorithm that is designed to protect data in transit between a BlackBerry device and the BlackBerry® Enterprise Server. Standard BlackBerry encryption, which is designed to provide strong security, helps protect data in transit to the BlackBerry Enterprise Server when message data is outside of the organization's firewall.

Standard BlackBerry encryption is designed to encrypt messages that a BlackBerry device sends or that the BlackBerry Enterprise Server forwards to the BlackBerry device. Standard BlackBerry encryption encrypts messages as follows:

- from the time the user sends an email message or PIN message from the BlackBerry device to the time when the BlackBerry Enterprise Server receives the message

- from the time the BlackBerry Enterprise Server receives a message to the time when the user opens the decrypted message on the BlackBerry device

Before the BlackBerry device sends a message, it compresses the message and then encrypts the message using the master encryption key, which is unique to that BlackBerry device. The BlackBerry device does not use the master encryption key in the compression process.

When the BlackBerry Enterprise Server receives the message from the BlackBerry device, the BlackBerry Dispatcher decrypts the message using the master encryption key of the BlackBerry device, and then decompresses the message.

How the BlackBerry Enterprise Server uses a Triple DES encryption algorithm

The BlackBerry® Enterprise Solution uses a two-key Triple DES encryption algorithm to create message keys and master encryption keys. In each of three iterations of the DES algorithm, the first of two 56-bit keys in outer CBC mode encrypts the data, the second key decrypts the data, and then the first key encrypts the data again. For more information, see *Federal Information Processing Standard - FIPS PUB 81 [3]*.

The BlackBerry Enterprise Solution stores the message keys and master encryption keys as 128-bit long binary strings, with each parity bit in the least significant bit of each of the 8 bytes of key data. The message keys and master encryption keys have overall key lengths of 112 bits and include 16 bits of parity data.

How the BlackBerry Enterprise Solution uses an AES encryption algorithm

The BlackBerry® Enterprise Solution uses an AES algorithm in CBC mode to create message keys and master encryption keys that contain 256 bits of key data.

The way that BlackBerry devices implement AES is designed to protect user data and encryption keys on BlackBerry devices from traditional attacks and side-channel attacks. Side-channel attacks can occur in the form of power analysis readings or electromagnetic radiation emissions.

BlackBerry devices implement AES in a way that uses countermeasures (for example, masking operations, table splitting, and applications of random masks) to hide the true operations taking place on the BlackBerry device. These countermeasures are designed to help protect the cryptographic keys and plain-text data against potential side-channel attacks at all points during the AES encryption and decryption operations so that the attacks do not reveal data that can expose the encryption key.

Options for extending messaging security

When a user sends a message from the BlackBerry® device, by default, the BlackBerry® Enterprise Server does not encrypt the message when it forwards the message to the message recipient. To extend the messaging security that standard BlackBerry encryption provides, the user must install additional secure messaging technology on the BlackBerry device, and you must set the BlackBerry device to use that secure messaging technology.

To offer an additional layer of messaging security between the sender and recipient of an email message or PIN message, you can turn on S/MIME technology or PGP® technology for BlackBerry devices. When you use either one of these technologies, you allow sender-to-recipient authentication and confidentiality. These technologies also help to maintain the integrity and privacy of the data from the time that a BlackBerry device user sends a message from the BlackBerry device to when the message recipient decrypts and opens the message.

Options for encrypting stored data

You can configure the BlackBerry® Enterprise Solution to encrypt the user data and encryption keys on locked BlackBerry devices.

Protection of user data on locked BlackBerry devices

When the content protection feature on BlackBerry® devices is turned on, the BlackBerry devices are designed to protect user data in the following ways:

- use 256-bit AES encryption to encrypt stored data
- use ECC public keys to encrypt data that the BlackBerry devices receive

User data that BlackBerry devices can encrypt when the content protection feature is turned on

Item	Description
AutoText	all text that automatically replaces the text that BlackBerry® device users type
BlackBerry® Browser	• content that web sites or third-party applications push to BlackBerry devices • web sites that users save on their BlackBerry devices • browser cache
calendar	• subject • location • meeting organizer • meeting participants • notes included in calendar items
address book contacts	all contact information except the contact title and category For information about using the Force Include Address Book In Content Protection IT policy rule to prevent users from turning off encryption for the address book, see the *BlackBerry Enterprise Server Policy Reference Guide*.
message list	• subject

Item	Description
	• email addresses • message body • attachments
memo list	• title • information included in the body of notes
Open Mobile Alliance™ DRM applications	keys that identify the BlackBerry devices and SIM cards (if available) that the BlackBerry devices add to DRM forward-locked applications
RSA SecurID® library	the contents of the .sdtid file seed that is stored in flash memory
tasks	• subject • information included in the body of tasks

Protection of master encryption keys on locked BlackBerry devices

If you turn on content protection of master encryption keys, BlackBerry® devices use grand master keys to encrypt the master encryption keys that are stored in flash memory, and the BlackBerry devices store the decrypted grand master keys in RAM.

When you, a user, or the password timeout locks a BlackBerry device, the BlackBerry device continues to receive data and does not free the memory that is associated with the grand master key. If the BlackBerry device is locked and receives data that is encrypted with a master encryption key, the BlackBerry device uses the decrypted grand master key to decrypt the required master encryption key that is stored in flash memory and receive the data.

Controlling BlackBerry device access to the BlackBerry Enterprise Server

To control which BlackBerry® devices can connect to the BlackBerry® Enterprise Server, you can turn on the Enterprise Service Policy. After you turn on the Enterprise Service Policy, by default, the BlackBerry Enterprise Server prevents connections from new BlackBerry devices that you associate with the BlackBerry Enterprise Server and permits connections from BlackBerry devices that you previously activated on the BlackBerry Enterprise Server. The Enterprise Service Policy also applies to devices with BlackBerry® Connect™ software or BlackBerry® Built-In™ software, and devices that are running the BlackBerry® Application Suite.

You can use the Enterprise Service Policy to create allowed lists that control the BlackBerry devices that users can activate on a BlackBerry Enterprise Server, over the wireless network, or over a serial connection. BlackBerry devices that match the criteria that you specify in the allowed list can complete the activation process on the BlackBerry Enterprise Server.

You can define individual BlackBerry device PINs and a range of BlackBerry device PINs as types of criteria in the allowed lists.

You can also control access to the BlackBerry Enterprise Server based on specific manufacturers and models of BlackBerry devices. The BlackBerry Administration Service includes lists of permitted manufacturers and models based on the properties of the BlackBerry devices that are already associated with the BlackBerry Enterprise Server. You can clear items in the allowed lists to prevent further connections by BlackBerry devices of a specific manufacturer or model.

You can permit a specific user to override the Enterprise Service Policy so that the user can connect to the BlackBerry Enterprise Server even if the user's BlackBerry device matches the criteria for BlackBerry devices to exclude.

Managing BlackBerry device security over the wireless network using IT administration commands

You can control BlackBerry® devices remotely to protect confidential information using IT administration commands.

Goal	Description
permanently delete application data on a lost or stolen BlackBerry device	If a BlackBerry device is lost or stolen, you can send the Erase data and disable BlackBerry device IT administration command to delete all information and application data from the BlackBerry device and make the BlackBerry device unavailable for use.
lock a misplaced BlackBerry device	If a BlackBerry device is misplaced but likely not lost or stolen, you can send the Set password and lock the BlackBerry device IT administration command to set a password and lock the BlackBerry device. You can also send this IT administration command if a user forgets the BlackBerry device password.
label a BlackBerry device with owner information	If a BlackBerry device is lost or stolen, you can send the Set owner information IT administration command so that owner information appears on the screen when the BlackBerry device is locked. The owner information might include contact information that the finder can use to return the BlackBerry device to the owner.

BlackBerry Monitoring Service

You can use the BlackBerry® Monitoring Service to monitor and troubleshoot issues with a BlackBerry® Enterprise Server in your organization's environment and to monitor the activity of the BlackBerry device users that are associated with the BlackBerry Enterprise Server.

The BlackBerry Monitoring Service monitors the BlackBerry Enterprise Server components. It polls each component and retrieves SNMP data that it stores in a database and displays in the BlackBerry Monitoring Service console.

Feature	Description
web-based administration console	You can use the BlackBerry Monitoring Service console to monitor a BlackBerry Enterprise Server in your organization's environment by creating thresholds that monitor the activity of BlackBerry Enterprise Server components. You can configure the BlackBerry Monitoring Service to send notification messages to contacts when a component's activity exceeds levels that you specify as acceptable. The BlackBerry Monitoring Service console provides configuration settings and statistics that you can use to review BlackBerry Enterprise Server activity.
monitoring of BlackBerry Enterprise Server components	The BlackBerry Monitoring Service can provide the following types of data: • configuration settings, such as the component name, component version, and computer name • statistics such as CPU usage, memory usage, number of requests to process, and number of processing threads • BlackBerry® Client Access License information, such as the number of used and available licenses • high availability information, such as the high availability status of components • policy information, such as the service books and IT policies that the BlackBerry Enterprise Server sends to BlackBerry devices • messaging statistics, such as the number of email messages that BlackBerry devices send and receive • messaging server information, such as the hung thread count • connection information for the BlackBerry Configuration Database, BlackBerry Controller, and SRP connections
BlackBerry device diagnostic tests and user monitoring	You can use the BlackBerry Monitoring Service console to run diagnostic tests for BlackBerry devices and identify any issues with BlackBerry devices. The BlackBerry device diagnostic tool is available for BlackBerry devices that are running BlackBerry® Device Software version 5.0 and later. The BlackBerry Monitoring Service can monitor the following types of data: • configuration information for BlackBerry devices, such as the PIN, network type, and phone number • message statistics, such as the pending and expired email messages, and email messages that BlackBerry devices send and receive

Feature	Description
	• BlackBerry device statistics, such as the battery level and network coverage
thresholds	You can define thresholds that you can use to monitor components and BlackBerry device users. When the activity of a component or BlackBerry device user that the BlackBerry Monitoring Service monitors reaches a threshold, the BlackBerry Monitoring Service displays an alarm in the BlackBerry Monitoring Service console and sends notification messages to specific contacts.
notification messages	You can configure the BlackBerry Monitoring Service to send notification messages to one or more recipients by creating a contact. A contact can include one or more email addresses, PINs, IP addresses, or phone numbers that support SMS text messages. If a component goes into an alarm state, the BlackBerry Monitoring Service sends a notification message to all of the recipients in the contact.
reports	You can run default reports or create custom reports to return data about the BlackBerry Enterprise Server instances in your organization's environment. You can export reports to a .csv, a .pdf, or an .html file. You can use the information that you collect from the reports to analyze historical data.
graphs	You can use the BlackBerry Monitoring Service console to generate a graph of a component's historical activity.
integration with a network management framework	The BlackBerry Monitoring Service can send notifications as SNMP trap messages. This permits you to integrate the BlackBerry Monitoring Service with a network management tool that can receive SNMP trap messages. The BlackBerry Monitoring Service sends an SNMP trap message when the activity of a component or BlackBerry device user that the BlackBerry Monitoring Service monitors reaches a threshold.

BlackBerry Threshold Analysis Tool

The BlackBerry® Threshold Analysis Tool is designed to reduce the effort it takes to create a threshold that you can use to monitor a data attribute of a BlackBerry® Enterprise Server component. The BlackBerry Threshold Analysis Tool creates thresholds that are appropriate for a data attribute based on the previous activity of the data attribute. You can run the tool instead of creating rules in the BlackBerry Monitoring Service console manually. You can run the tool using a command prompt on the computer that hosts the BlackBerry Monitoring Service. The tool creates rules in the BlackBerry Monitoring Service console. You can change or delete the rules.

You install the tool when you install the BlackBerry Monitoring Service.

BlackBerry Router

The BlackBerry® Router connects to the wireless network. It sends data to and receives data from the BlackBerry® Infrastructure for a BlackBerry® Enterprise Server.

The BlackBerry Router also sends data to and receives data from BlackBerry devices that are connected to the BlackBerry Enterprise Server using the BlackBerry® Device Manager.

You can install the BlackBerry Router on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server to route data between the BlackBerry Infrastructure and one or more BlackBerry Enterprise Server instances.

BlackBerry Policy Service

The BlackBerry® Policy Service sends IT policies and IT administration commands to BlackBerry devices and provisions service books over the wireless network. When you activate a BlackBerry device, change an IT policy, or request that a BlackBerry® Enterprise Server resend service books, the BlackBerry Enterprise Server uses the BlackBerry Policy Service to send the updates to the BlackBerry device.

An IT policy consists of rules that define BlackBerry device security, settings for synchronizing data over the wireless network, and other behaviors for the individual groups or user accounts that you define. You can configure IT policies using the BlackBerry Administration Service.

Feature	Description
wireless delivery	When you configure an IT policy, all rules take effect when the BlackBerry Policy Service delivers the IT policy to a BlackBerry device over the wireless network. The BlackBerry device stores new IT policy rule values in the user configurations on the BlackBerry device automatically. To keep the IT policy rules current, a BlackBerry Enterprise Server sends the IT policy to the BlackBerry device over the wireless network periodically.
IT policy coverage	When you add a user account to a BlackBerry Enterprise Server, the BlackBerry Policy Service applies the Default IT policy to the user account automatically. The user account is not active on the BlackBerry Enterprise Server until a BlackBerry device accepts the IT policy. You can apply a different IT policy to a user account. If you delete an IT policy that you applied to a user account, the BlackBerry Policy Service applies the user account to the Default IT policy automatically.

Feature	Description
IT policy assignment	You can apply an IT policy to a group or an individual user account.
resend options	If a BlackBerry Enterprise Server cannot send an updated IT policy to a BlackBerry device immediately (for example, if a user is outside of a wireless coverage area), you can resend the IT policy manually or configure when the BlackBerry Policy Service resends the IT policy. The BlackBerry Enterprise Server continues to resend the IT policy until it delivers the IT policy.
security enforcement	You can configure IT polices that define security settings for BlackBerry devices, the BlackBerry® Desktop Software and the BlackBerry® Web Desktop Manager, and that override security settings that users define on their BlackBerry devices. For example, you can configure whether a password is required for a BlackBerry device, the length of time that the password can exist before it becomes invalid, and the length and composition of the password. You can also use IT policies to specify encryption key details.

BlackBerry Configuration Panel

The BlackBerry® Configuration Panel displays data, such as BlackBerry Configuration Database settings, that the BlackBerry® Enterprise Server setup application gathered during the installation process. You can use the BlackBerry Configuration Panel to change configuration data after you install the BlackBerry Enterprise Server.

BlackBerry Administration Service

The BlackBerry® Administration Service is a web application you can use to manage user accounts; assign user groups, administrative roles, and software configurations and apply IT policies to user accounts; and manage servers and component instances in a BlackBerry Domain. You can open the BlackBerry Administration Service in a browser on any computer that can access the computer that hosts the BlackBerry Administration Service. You can share administrative duties with multiple administrators who can access the BlackBerry Administration Service simultaneously using unique user names and passwords. When Microsoft® ActiveX® controls are turned on in your browser, you can connect BlackBerry devices to your computers and manage the BlackBerry devices while you are logged in to the BlackBerry Administration Service.

Feature	Description
high availability of BlackBerry Enterprise Server components	You can install standby instances of BlackBerry® Enterprise Server components and configure a manual or automatic failover to a standby instance.

Feature	Description
ability to assign users to multiple groups	Groups permit you to share administrative roles, IT policies, and other configuration settings among similar user accounts so that properties can be set once instead of for every user. You can assign a user account to more than one group so that the user inherits the properties of every group that the user belongs to. You can also assign groups to other groups to share the properties of the parent group with all of the user accounts in the child groups.
custom server and component names using friendly names	To help you identify servers and component instances, you can define a friendly name for each BlackBerry Enterprise Server and component instance that displays in the BlackBerry Administration Service. Each regional language that the BlackBerry Administration Service supports can have unique friendly names.
custom administrative roles	Each action that you perform in the BlackBerry Administration Service is associated with a privilege. You can specify the actions that administrators can perform by changing the privilege that you assign to administrative roles.
BlackBerry Administration Service authentication or external authentication	Administrators that log in to the BlackBerry Administration Service must provide their user names and passwords. A user name and a password is a unique combination that is stored securely in the BlackBerry Configuration Database and known only to the BlackBerry Administration Service. Alternatively, you can use external authentication, which permits administrators to log in to the BlackBerry Administration Service using the same information that administrators use to access your organization's messaging server.
options for viewing the BlackBerry Domain	You can find and manage BlackBerry Enterprise Server component instances using the server view or component view.

BlackBerry Web Desktop Manager

The BlackBerry® Web Desktop Manager is a web application that provides many of the same features that the BlackBerry® Desktop Manager does. Users can connect their BlackBerry devices to their computers using a USB connection or Bluetooth® connection, and log in to BlackBerry Web Desktop Manager to activate and manage their BlackBerry devices, back up and restore data, define email settings, and update the BlackBerry® Device Software.

Feature	Description
access	Users can access device management and configuration capabilities from any computer that can access the intranet.

Feature	Description
application management	Users can use the BlackBerry Web Desktop Manager to install, manage, and remove the applications that are installed on their BlackBerry devices.
BlackBerry Device Software management	Users can use the BlackBerry Web Desktop Manager to update the BlackBerry Device Software on their BlackBerry devices.
control user's access to features	You can specify the BlackBerry Web Desktop Manager features that users can access using IT policies and settings in the BlackBerry Administration Service.
customizable interface	You can customize the appearance of the UI to match your organization's requirements. You can customize the font colors, logo, and the help.
device activation	Users can use the BlackBerry Web Desktop Manager to set activation passwords and activate their BlackBerry devices.
switch devices	Users can use the BlackBerry Web Desktop Manager to switch BlackBerry devices, and migrate from third-party devices that have BlackBerry® Application Suite installed, to BlackBerry devices.
folder redirection	Users can use the BlackBerry Web Desktop Manager to select the folders that the BlackBerry® Enterprise Server redirects messages from.
language support	The BlackBerry Web Desktop Manager is available in English, French, German, Italian, Spanish, and Japanese. Users can select a language before they log in to the BlackBerry Web Desktop Manager.
simplified administration	The web UI does not require you to deploy, support, and maintain client-side software such as the BlackBerry Desktop Manager.
service statistics	The BlackBerry Web Desktop Manager provides users with statistics about the message status (forwarded, sent, pending, expired, filtered), last contact time, and information about the last message sent or received.
synchronization of contact folders	Users can use the BlackBerry Web Desktop Manager to select the public or private contact folders that they want to synchronize to their BlackBerry devices over the wireless network.

Comparison of BlackBerry Web Desktop Manager and BlackBerry Desktop Manager features

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Manager
ability to view the BlackBerry® Desktop Software that is installed on the users' computers	supported	supported
application loader tool	supported with the following conditions: • option to choose not to save the backup file • BlackBerry services are not maintained if the users disconnect their BlackBerry devices before completing the process	supported with the following conditions: • no option to choose whether to save the backup file • BlackBerry services are maintained if the users disconnect their BlackBerry devices before clicking the Close button in the Load was successful dialog box
BlackBerry® Desktop Redirector	not included	included
BlackBerry® Device Software updates	supported with the following conditions: • you install the software on a shared network drive • BlackBerry® Web Desktop Manager forces users to update the BlackBerry® Device Software when a software configuration is assigned to the user accounts	supported with the following conditions: • users install the software on their computers and run the application loader tool • BlackBerry Desktop Manager notifies the users when a newer version of BlackBerry Device Software is available on their computers
certificate synchronization	not supported	supported
changing the email profile options	not supported	supported
connections to BlackBerry devices	supported with the following conditions: • users can connect to multiple BlackBerry devices at the same time	supported with the following conditions: • users can connect to only one BlackBerry device at a time

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Manager
	• BlackBerry Web Desktop Manager does not prompt users if they want to switch from using a Bluetooth® connection to using a USB connection	• BlackBerry Desktop Manager prompts users if they want to switch from using a Bluetooth connection to using a USB connection
device activation	supported with the following conditions: • occurs automatically for new users • if users without active BlackBerry devices connect BlackBerry devices that belong to other users, the BlackBerry Web Desktop Manager prompts the users who connected the BlackBerry devices if they want to switch to the BlackBerry devices	supported with the following conditions: • occurs automatically each time users plug in a BlackBerry device • if users without active BlackBerry devices connect BlackBerry devices that belong to other users, the BlackBerry Desktop Manager notifies the users who connected the BlackBerry devices that an activation process is underway by asking the users whether an encryption key should be created
switching devices	supported with the following conditions: • users can switch from third-party devices that are running BlackBerry® Application Suite to BlackBerry devices • users can switch between BlackBerry devices • BlackBerry services are not maintained if users disconnect their BlackBerry devices before completing the process	supported with the following conditions: • users can switch from third-party devices to BlackBerry devices • BlackBerry services are maintained if users disconnect their BlackBerry devices before clicking the Close button in the Switch was successful dialog box
email message settings	supported with the following conditions: • users can import data from the address book when creating or changing a filter	supported with the following conditions: • users can import data for filtering • users can turn off message redirection while their BlackBerry device are connected

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Manager
	• users cannot turn off message redirection while their BlackBerry devices are connected • users cannot generate encryption keys • users cannot override email addresses	• users can generate encryption keys • users can override email addresses
media management	not supported	supported
modem support for devices	not supported	supported
prompt for BlackBerry device password	BlackBerry devices can connect without a prompt for the device password	required before BlackBerry devices can connect to the users' computers
statistics for user accounts	supported with the following conditions: • all supported messaging environments • users cannot clear the redirection queue • users cannot clear the redirection statistics	supported with the following conditions: • Microsoft® Exchange environments only • users can clear the redirection queue • users can clear the redirection statistics
supported BlackBerry Device Software versions	BlackBerry Device Software version 4.0 and later	all
supported IT policies	• Auto Backup Enabled • Auto Backup Exclude Messages • Auto Backup Exclude Sync • Auto Backup Frequency • Auto Backup Include All • Desktop Allow Device Switch • Desktop Password Cache Timeout • Do Not Save Sent Messages • Force Load Message	• Auto Backup Enabled • Auto Backup Exclude Messages • Auto Backup Exclude Sync • Auto Backup Frequency • Auto Backup Include All • Desktop Allow Device Switch • Desktop Password Cache Timeout • Disable Media Manager • Do Not Save Sent Messages • Force Load Count • Forward Message In Cradle • Message Prompt

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Manager
		• Show AppLoader • Show Web Link
synchronization over a serial connection	users cannot synchronize the following data over a serial connection: • organizer data • email messages • third-party application data • date and time	users can synchronize the following data over a serial connection: • organizer data • email messages • third-party application data • date and time

BlackBerry Enterprise Server high availability

4

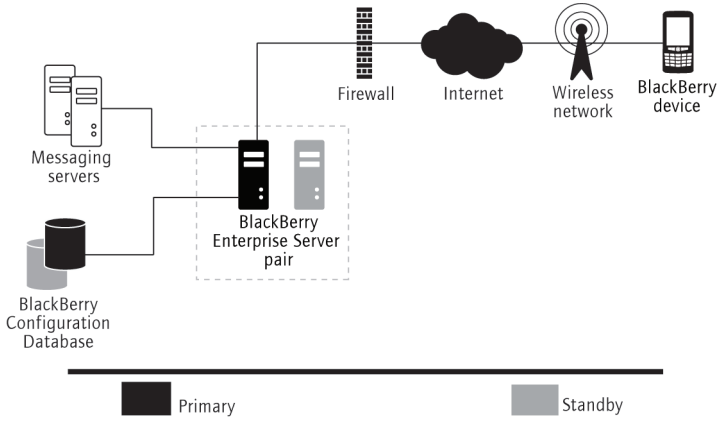
High availability permits you to provide minimum downtime for BlackBerry® services if BlackBerry® Enterprise Server components stop responding or if they require maintenance. BlackBerry Enterprise Server high availability consists of a minimum of two BlackBerry Enterprise Server instances and the BlackBerry Configuration Database which is replicated across two database servers. High availability is designed so that no single point of failure exists in the BlackBerry® Enterprise Solution that could break the messaging and application data flow to and from BlackBerry devices.

When you configure the BlackBerry Enterprise Server for high availability, you install a primary BlackBerry Enterprise Server and a standby BlackBerry Enterprise Server on different computers within the same network segment. These BlackBerry Enterprise Server instances create a BlackBerry Enterprise Server pair. Both BlackBerry Enterprise Server instances use the same SRP credentials and BlackBerry Configuration Database. You can configure the failover process to be automatic or manual.

The standby BlackBerry Enterprise Server connects to the primary BlackBerry Enterprise Server and checks periodically that the primary BlackBerry Enterprise Server is healthy. The health of a BlackBerry Enterprise Server is determined by thresholds that you can configure. If the health of the primary BlackBerry Enterprise Server falls below the failover threshold or if the primary BlackBerry Enterprise Server stops responding, the standby BlackBerry Enterprise Server tries to promote itself. If the messaging server and the BlackBerry Configuration Database remain available during the failover process, the message delays that users might experience are similar to the delays that users experience when you start a BlackBerry Enterprise Server instance.

BlackBerry Enterprise Server high availability in a small-scale environment

The following diagram shows how you can configure a BlackBerry® Enterprise Server for high availability in a small-scale environment. Each primary BlackBerry Enterprise Server instance requires its own standby BlackBerry Enterprise Server instance. You install the primary BlackBerry Enterprise Server and standby BlackBerry Enterprise Server on different computers. You can install all BlackBerry Enterprise Server components on both computers to minimize the number of computers that the BlackBerry Enterprise Server environment requires.



Both BlackBerry Enterprise Server instances in the BlackBerry Enterprise Server pair include, by default, the BlackBerry Attachment Service, BlackBerry Dispatcher, BlackBerry MDS Connection Service, BlackBerry Messaging Agent, BlackBerry Policy Service, BlackBerry Router, and BlackBerry Synchronization Service. By default, if you choose to install the BlackBerry Collaboration Service with both instances, the BlackBerry Collaboration Service is included in the BlackBerry Enterprise Server pair.

To administer the BlackBerry Enterprise Server pair, you can install the BlackBerry Administration Service with both BlackBerry Enterprise Server instances and configure high availability for the BlackBerry Administration Service separately.

In a large-scale environment, you can add any number of BlackBerry Enterprise Server pairs that use the same BlackBerry Configuration Database.

How the BlackBerry Enterprise Server calculates health scores

Certain BlackBerry® Enterprise Server components calculate a health score that indicates how well the component can provide specific services. The components send their health scores to the BlackBerry Dispatcher, which combines the health scores of the components to calculate the overall health score of the BlackBerry Enterprise Server. The BlackBerry Dispatcher writes the information to the BlackBerry Configuration Database, and it provides the information to a BlackBerry Enterprise Server that requests it.

The BlackBerry Enterprise Server components calculate their health scores by examining their operating health, the stability of their connections to other components, and the health scores of the other components.

The health score of the BlackBerry Enterprise Server consists of various health parameters. Each health parameter indicates whether a particular service or feature is available. If you turn on the automatic failover feature for the BlackBerry Enterprise Server, you can configure health parameters so that the BlackBerry Enterprise Server fails over automatically when critical services or features are no longer available.

Conditions for failover to a standby BlackBerry Enterprise Server

Failover between the primary and standby BlackBerry® Enterprise Server instances occurs when the standby BlackBerry Enterprise Server determines that its health score is above the promotion threshold and one or more of the following events occurred:

- The standby BlackBerry Enterprise Server receives a health score from the primary BlackBerry Enterprise Server that is below the failover threshold.
- The standby BlackBerry Enterprise Server reads, in the BlackBerry Configuration Database, a health score for the primary BlackBerry Enterprise Server that is below the failover threshold.
- The standby BlackBerry Enterprise Server does not receive a response when it checks the BlackBerry Dispatcher for the health score of the primary BlackBerry Enterprise Server.
- The standby BlackBerry Enterprise Server pings the BlackBerry Dispatcher on the network but cannot determine whether the primary BlackBerry Enterprise Server is running.

How a primary BlackBerry Enterprise Server demotes itself

After the primary BlackBerry® Enterprise Server receives a request to demote itself from a standby BlackBerry Enterprise Server, the primary BlackBerry Enterprise Server performs the following actions:

- closes its SRP connection to the BlackBerry® Infrastructure
- stops the flow of all messages
- demotes its connections to the messaging server and BlackBerry Configuration Database to standby connections
- informs the standby BlackBerry Enterprise Server that it demoted itself

Scenario: What happens after a primary BlackBerry Enterprise Server stops responding

If a primary BlackBerry® Enterprise Server stops responding, the response of the standby BlackBerry Enterprise Server depends on whether its health score is above or below the promotion threshold.

The following responses assume that the messaging server, BlackBerry® Infrastructure, and BlackBerry Configuration Database are available.

Response of the standby BlackBerry Enterprise Server when its health score is above the promotion threshold

1. The standby BlackBerry Enterprise Server determines that the primary BlackBerry Enterprise Server stopped responding.
2. The standby BlackBerry Enterprise Server checks its health score and determines that the health score is above the promotion threshold.
3. The standby BlackBerry Enterprise Server opens active connections to the BlackBerry Configuration Database and messaging server.
4. The standby BlackBerry Enterprise Server tries to open an SRP connection to the BlackBerry Infrastructure.
5. When the connection to the BlackBerry Infrastructure is stable, the standby BlackBerry Enterprise Server writes its identity as the primary BlackBerry Enterprise Server to the BlackBerry Configuration Database.

Response of the standby BlackBerry Enterprise Server when its health score is below the promotion threshold

1. The standby BlackBerry Enterprise Server determines that the primary BlackBerry Enterprise Server stopped responding.
2. The standby BlackBerry Enterprise Server checks its health score and determines that the health score is below the promotion threshold.

   The standby BlackBerry Enterprise Server cannot become the primary instance. You must resolve any issues before the BlackBerry Enterprise Server can recover.

Scenario: What happens after the health score of a primary BlackBerry Enterprise Server falls below the failover threshold

The following scenario assumes that the messaging server, BlackBerry® Infrastructure, and BlackBerry Configuration Database are available.

1. The standby BlackBerry® Enterprise Server determines that the health score of the primary BlackBerry Enterprise Server fell below the failover threshold.
2. The standby BlackBerry Enterprise Server checks its health score and determines that its health score is above the promotion threshold and higher than the health score of the primary BlackBerry Enterprise Server.
3. The standby BlackBerry Enterprise Server sends a demotion request to the pimary BlackBerry Enterprise Server.
4. The primary BlackBerry Enterprise Server demotes itself.
5. The standby BlackBerry Enterprise Server opens active connections to the BlackBerry Configuration Database and messaging server.
6. The standby BlackBerry Enterprise Server tries to open an SRP connection to the BlackBerry Infrastructure.
7. The standby BlackBerry Enterprise Server writes its identity as the primary BlackBerry Enterprise Server to the BlackBerry Configuration Database.

BlackBerry Configuration Database high availability

The type of BlackBerry® Configuration Database high availability that you can configure depends on the type of database server that is in your organization's environment.

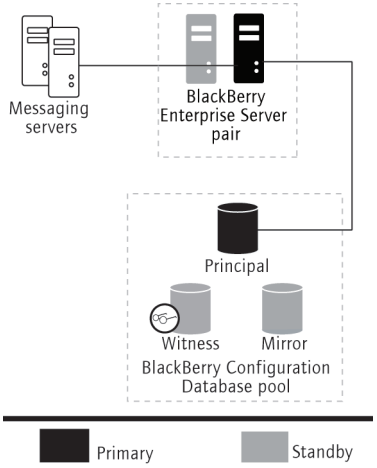
If your organization's environment includes Microsoft® SQL Server® 2005 SP2 or later, you can configure database mirroring. Database mirroring requires a principal database, mirror database, and, optionally, a witness. Although the BlackBerry® Enterprise Server can contact the mirror database, it opens active connections to the principal database only. If the principal database stops responding, the BlackBerry Enterprise Server opens an active connection to the mirror database automatically. Database mirroring provides fault tolerance for the BlackBerry® Enterprise Solution.

If your organization's environment includes a version of Microsoft SQL Server that is earlier than version 2005 SP2, you can configure transactional replication of the BlackBerry Configuration Database and create a replicated BlackBerry Configuration Database. If the BlackBerry Configuration Database stops responding, you must fail over the BlackBerry Enterprise Server to the replicated BlackBerry Configuration Database manually.

For more information about database mirroring, visit www.microsoft.com.

BlackBerry Configuration Database mirroring

The following diagram shows how you can configure the BlackBerry® Configuration Database with principal and mirror instances for high availability. The BlackBerry Configuration Database supports an optional witness. The BlackBerry® Enterprise Server connects to the principal BlackBerry Configuration Database directly, and can fail over to the mirror BlackBerry Configuration Database if the principal BlackBerry Configuration Database stops responding.



The primary BlackBerry Enterprise Server connects to the principal BlackBerry Configuration Database and accesses data from it. The name of the mirror BlackBerry Configuration Database is stored in the Windows® registry of the computers that hosts the primary and standby BlackBerry Enterprise Server instances. The BlackBerry Enterprise Server instances do not connect to the mirror BlackBerry Configuration Database until after the principal BlackBerry Configuration Database stops responding.

The primary BlackBerry Enterprise Server connects to the messaging server and processes the messaging data that it sends to and receives from BlackBerry devices.

The standby BlackBerry Enterprise Server opens standby connections to the principal BlackBerry Configuration Database and the messaging server.

Scenario: What happens after the principal BlackBerry Configuration Database stops responding

If a principal BlackBerry® Configuration Database stops responding, the response of the primary BlackBerry® Enterprise Server depends on whether it can connect to the mirror BlackBerry Configuration Database.

The following responses assume that the messaging server and BlackBerry® Infrastructure are available.

Response of a primary BlackBerry Enterprise Server that can connect to the mirror BlackBerry Configuration Database

1. The primary BlackBerry Enterprise Server loses its connection to the principal BlackBerry Configuration Database.
2. The primary BlackBerry Enterprise Server connects to the mirror BlackBerry Configuration Database.
3. The primary BlackBerry Enterprise Server remains the primary instance.

Response of a primary BlackBerry Enterprise Server that cannot connect to the mirror BlackBerry Configuration Database

1. The primary BlackBerry Enterprise Server loses its connection to the principal BlackBerry Configuration Database.
2. The primary BlackBerry Enterprise Server tries to connect to the mirror BlackBerry Configuration Database, but is unsuccessful.
3. The primary BlackBerry Enterprise Server lowers its health score and continues to provide limited services.
   One of the following events occurs:
   - If the standby BlackBerry Enterprise Server can open a connection to the principal or mirror BlackBerry Configuration Database, it demotes the primary BlackBerry Enterprise Server and promotes itself to become the primary instance.
   - If the standby BlackBerry Enterprise Server cannot open a connection to the principal or mirror BlackBerry Configuration Database, it cannot promote itself. You must resolve any issues before the BlackBerry Enterprise Server pair can recover.

High availability in a distributed environment

If you install multiple BlackBerry® Enterprise Server components on different computers to create a distributed environment, you can configure the components for high availability. High availability for a distributed component requires that you install two or more instances of the component in your organization's environment. When an instance stops responding, the other instances can take over.

When you install multiple BlackBerry Enterprise Server components in a distributed environment, each BlackBerry Enterprise Server component implements high availablility differently.

Component	High availability type	Description
BlackBerry Administration Service	load balancing using DNS round robin, or a hardware load balancer	When you install two or more BlackBerry Administration Service instances, you can create a BlackBerry Administration Service pool. You can access the BlackBerry Administration Service instances using a single web address. The load is distributed across the instances. If a BlackBerry Administration Service instance stops responding, the pool routes requests to the available instances.

Component	High availability type	Description
BlackBerry Attachment Service	load-balancing with primary and secondary groups	When you install two or more BlackBerry Attachment Service instances, you can create a BlackBerry Attachment Service pool for each BlackBerry Enterprise Server instance. You can configure a pool with a primary group of instances and, optionally, a secondary group of instances. The BlackBerry Enterprise Server sends all requests to the primary group. If the primary group cannot convert a specific file format, the BlackBerry Enterprise Server forwards conversion requests for the specific file format to the secondary group.
BlackBerry Collaboration Service	failover with an active connection to one instance and standby connections to other instances	When you install two or more BlackBerry Collaboration Service instances, you can create a BlackBerry Collaboration Service pool for each BlackBerry Enterprise Server instance. Each BlackBerry Enterprise Server assigns one of the connections to the BlackBerry Collaboration Service instances as the active connection, and the other connections as standby connections. If the BlackBerry Collaboration Service that the active connection is assigned to stops responding, the BlackBerry Enterprise Server assigns the active connection to another BlackBerry Collaboration Service instance.
BlackBerry Configuration Database	database mirroring	If you install the BlackBerry Configuration Database on Microsoft® SQL Server® 2005 SP2 or later, you can configure database mirroring. If the principal BlackBerry Configuration Database stops responding, the BlackBerry Enterprise Server fails over to the mirror BlackBerry Configuration Database.
BlackBerry MDS Connection Service	failover with an active connection to one instance and standby connections to other instances	When you install two or more BlackBerry MDS Connection Service instances, you can create a BlackBerry MDS Connection Service pool for each BlackBerry Enterprise Server instance. Each BlackBerry Enterprise Server assigns one of the connections to the BlackBerry MDS Connection Service instances as the active connection, and the other connections as standby connections. If the BlackBerry MDS Connection Service that the active connection is assigned to stops

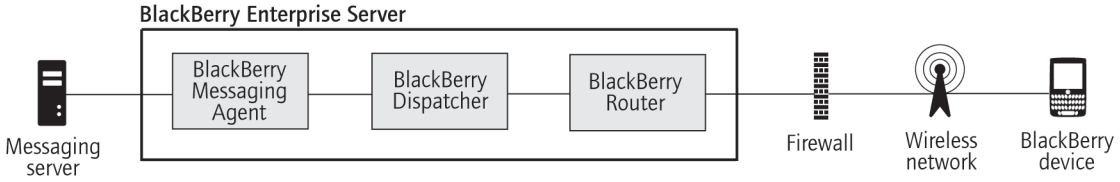
Component	High availability type	Description
		responding, the BlackBerry Enterprise Server assigns the active connection to another BlackBerry MDS Connection Service instance.
BlackBerry MDS Integration Service	load balancing with DNS round robin or a hardware load balancer	When you install two or more BlackBerry MDS Integration Service instances, you can create a BlackBerry MDS Integration Service pool using DNS round robin or a hardware load balancer. If a BlackBerry MDS Integration Service instance stops responding, DNS round robin or the hardware load balancer redistributes requests to the available instances.
BlackBerry Monitoring Service	none	The BlackBerry Monitoring Service does not support high availability. If you install two or more BlackBerry Monitoring Service instances in your organization's environment, only the first instance is used. To use another BlackBerry Monitoring Service instance, you can switch to the instance manually using the BlackBerry Configuration Panel.
BlackBerry Router	failover	When you install two or more BlackBerry Router instances, you can create a BlackBerry Router pool for each BlackBerry Enterprise Server or BlackBerry Enterprise Server pair. If a BlackBerry Router stops responding, the BlackBerry Enterprise Server selects another instance using information that is stored in the BlackBerry Configuration Database.

BlackBerry Enterprise Server process flows

5

Messaging process flows

Process flow: Sending a message to a BlackBerry device



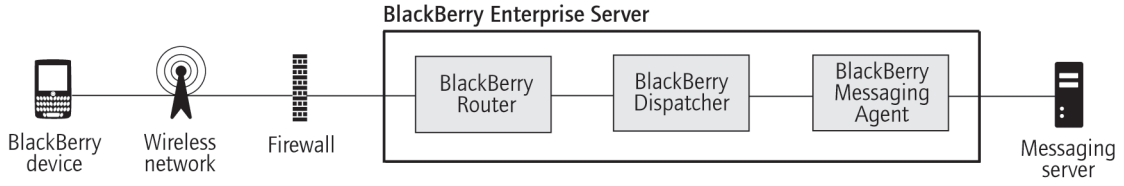
1. A message arrives in a user's mailbox. Microsoft® Exchange notifies the BlackBerry® Messaging Agent.
2. The BlackBerry Messaging Agent applies global filter rules to the messages in the user's mailbox and filters the messages that match the filter criteria.

   If no global filter rules apply, the BlackBerry Messaging Agent applies filter rules that are user defined to the messages in the user's mailbox.
3. The BlackBerry Messaging Agent sends the first 2 KB of the message to the BlackBerry Dispatcher.
4. The BlackBerry Dispatcher compresses the first 2 KB of the message, encrypts it using the master encryption key of the BlackBerry device, and sends the encrypted data to the BlackBerry Router.
5. The BlackBerry Router sends the encrypted data to the wireless network over port 3101, or over port 4101 if the BlackBerry device is a Wi-Fi® enabled BlackBerry device that is connected to the enterprise Wi-Fi network.
6. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network, and sends the message data to the BlackBerry device.
7. The BlackBerry device sends a delivery confirmation to the BlackBerry Dispatcher. The BlackBerry Dispatcher sends the delivery confirmation to the BlackBerry Messaging Agent.

   If the BlackBerry Messaging Agent does not receive a delivery confirmation within four hours, it sends the message to the wireless network again.

   The delivery confirmation verifies that the wireless network delivered the message to the BlackBerry device, but it does not verify that the user received or opened the message.
8. The BlackBerry device decrypts and decompresses the message so that the user can view it, and notifies the user that the message has arrived.

Process flow: Sending a message from a BlackBerry device



This process flow applies to new messages, reconciled messages (messages that a user moved, deleted, or marked as read or unread), and wireless calendar entries.

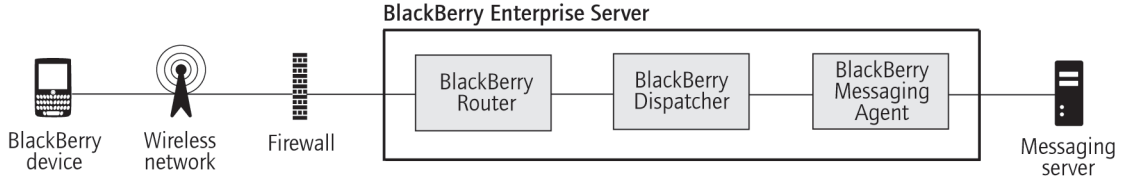
1. A user sends a message from a BlackBerry® device.

   The BlackBerry device assigns a RefId to the message. If the message is a meeting invitation or calendar entry, the BlackBerry device appends the calendar information to the message. The BlackBerry device compresses and encrypts the message, and sends the message to the wireless network over port 3101, or over port 4101 if the BlackBerry device is a Wi-Fi® enabled BlackBerry device that is connected to the enterprise Wi-Fi network.
2. The wireless network sends the message to the BlackBerry® Enterprise Server.

   The BlackBerry Enterprise Server accepts only encrypted messages from the BlackBerry device.
3. The BlackBerry Dispatcher uses the master encryption key of the BlackBerry device to decrypt and decompress the message.

   If the BlackBerry Dispatcher cannot decrypt the message using the master encryption key, the BlackBerry Enterprise Server ignores the message and sends an error message to the BlackBerry device.
4. The BlackBerry Messaging Agent sends the message to the user's email application.
5. The BlackBerry Messaging Agent sends a copy of the message to the Sent Items view in the user's email application.
6. The messaging server delivers the message to the recipients.

Process flow: Sending a message that contains an attachment from a BlackBerry device



1. A user attaches a file to a message on a BlackBerry® device and sends the message.

- If the BlackBerry device is not running BlackBerry® Device Software version 4.2 or later, and if the BlackBerry device does not have a CMIME service book that indicates that the BlackBerry® Enterprise Server supports attachment uploads, the Add Attachment menu item does not appear on the BlackBerry device.
- If the user tries to attach a file that exceeds the maximum file size that you specified, a notification appears and the user cannot attach the file.

2. The BlackBerry device compresses and encrypts the message, and sends the message to the wireless network over port 3101.

   The BlackBerry device formats the header of the message to indicate that a large attachment is part of the message. The BlackBerry device does not send the attachment content.
3. The wireless network sends the message to the BlackBerry Enterprise Server.
4. The BlackBerry Dispatcher decrypts and decompresses the message using the master encryption key of the BlackBerry device.

   If the BlackBerry Dispatcher cannot decrypt the message using the master encryption key, the BlackBerry Enterprise Server ignores the message and sends an error message to the BlackBerry device.
5. The BlackBerry Messaging Agent stores the message properties in the user's mailbox.

   The BlackBerry Messaging Agent sends a request for the attachment content through the BlackBerry Dispatcher to the BlackBerry device.
6. The BlackBerry device sends the attachment content through the BlackBerry Dispatcher to the BlackBerry Messaging Agent.

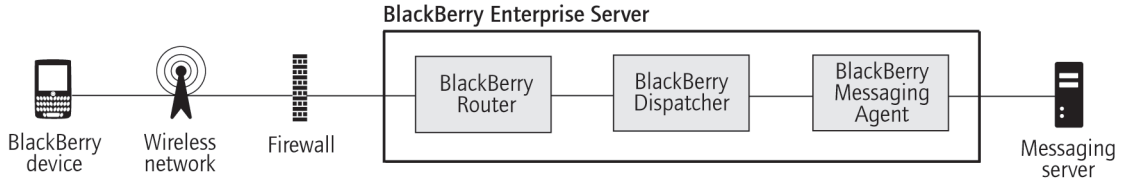
   If the file size of the attachment content exceeds a single data packet, the BlackBerry device divides the content into multiple data packets and sends the data packets to the BlackBerry Messaging Agent.
7. The BlackBerry Messaging Agent verifies the validity of the attachment content, and stores the content in memory as the content arrives.

   During the delivery of the attachment content, if the BlackBerry Messaging Agent does not receive content from the BlackBerry device for 15 minutes, the BlackBerry Messaging Agent cancels the message, deletes the partial attachment content from temporary storage, and sends an error message to the BlackBerry device.

   After all of the attachment content arrives, the BlackBerry Messaging Agent checks for other attachments that might be part of the same message.
   - If other attachments exist, the BlackBerry Messaging Agent requests the attachment content.
   - If no additional attachments exist, the BlackBerry Messaging Agent finishes processing the message and sends the message to the user's email application.

   The messaging server delivers the message to the intended recipients.

Process flow: Searching an organization's address book from a BlackBerry device



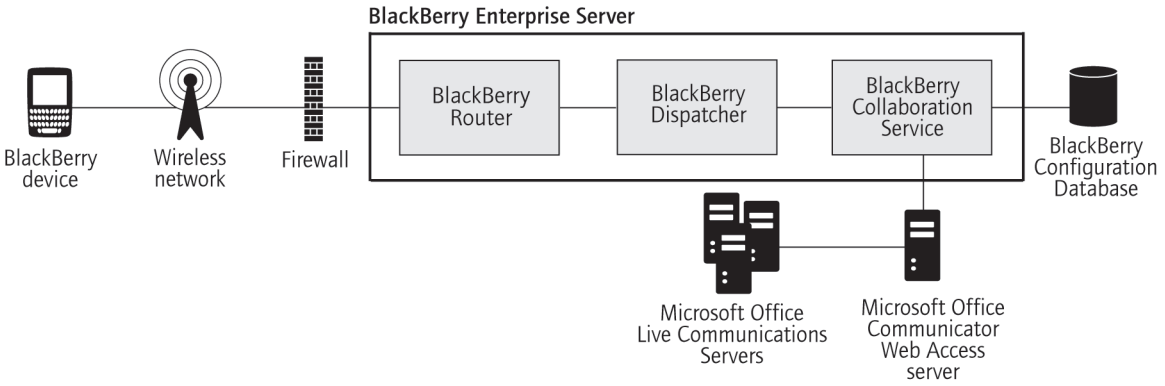
1. A user searches for a contact on a BlackBerry® device.
2. The BlackBerry device assigns a RefId to the search request, compresses and encrypts the request, and sends the request to the BlackBerry® Enterprise Server over port 3101.
3. The BlackBerry Dispatcher decrypts and decompresses the request using the master encryption key of the BlackBerry device, and sends the request to the BlackBerry Messaging Agent.
4. The BlackBerry Messaging Agent searches the GAL on the Microsoft® Exchange server and retrieves the 20 closest matches for the contact lookup request.

   The BlackBerry Messaging Agent sends the contact lookup results to the BlackBerry Dispatcher.
5. The BlackBerry Dispatcher encrypts the results using the master encryption key of the BlackBerry device, compresses the encrypted data, and sends it to the BlackBerry Router for delivery to the BlackBerry device.
6. The BlackBerry Router sends the encrypted data to the wireless network over port 3101.
7. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network, and sends the encrypted data to the BlackBerry device.
8. The BlackBerry device sends a delivery confirmation to the BlackBerry Dispatcher, which sends it to the BlackBerry Messaging Agent.

   If the BlackBerry Enterprise Server does not receive a delivery confirmation within four hours, it resubmits the contact lookup results to the wireless network.
9. The BlackBerry device decrypts and decompresses the contact lookup results with the master encryption key so that the user can view them on the BlackBerry device or add them to the contact list on the BlackBerry device.

Instant messaging process flows

Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Live Communications Server 2005 (Microsoft Office Communicator)



1. A user logs in to a collaboration client on a BlackBerry® device.
2. The BlackBerry device compresses and encrypts the user ID and password, and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion® proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
   - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on BlackBerry devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
   - If no idle sessions exist, the BlackBerry Collaboration Service sends a "Server Busy" status message to the BlackBerry device and rejects the login request.
   - If the maximum number of sessions is not set and the number of sessions equals the total number that the HTTP persistent connection supports, the BlackBerry Collaboration Service sends a "Failed" status message to the BlackBerry device and rejects the login request.

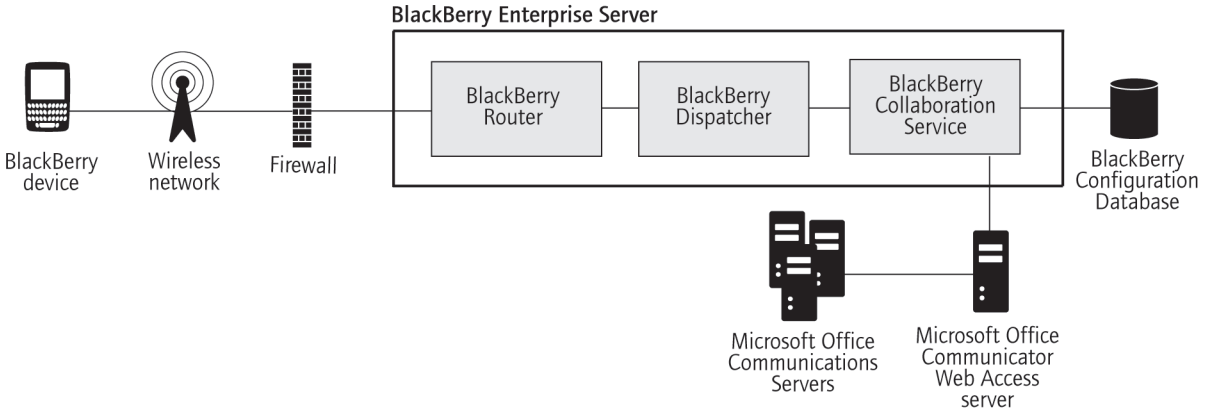
The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and tries to authenticate the user using Integrated Windows® Authentication. If the authentication is not successful, the BlackBerry Collaboration Service tries a forms-based login process instead. The BlackBerry Collaboration Service sends a login request in JSON, a lightweight data-interchange format, to the Microsoft® Office Communicator Web Access Server.

The BlackBerry Collaboration Service opens the connection using HTTPS over port 443. You can also configure the connection to use HTTP, the transport protocol that the AJAX service uses, or a custom port number.

5. The Microsoft Office Communicator Web Access server formats the request using a Microsoft API and sends the request to the Microsoft® Office Live Communications Server over an MTLS connection.
6. The Microsoft Office Live Communications Server accepts the request, processes the login information, and sends the acceptance to the Microsoft Office Communicator Web Access server.
7. The Microsoft Office Communicator Web Access server sends the acceptance to the BlackBerry Collaboration Service.
8. The BlackBerry Collaboration Service sends the acceptance, in encrypted and compressed format, through the BlackBerry Dispatcher to the BlackBerry device, and creates a cache of the connectivity information to maintain the instant messaging session.
9. The collaboration client on the BlackBerry device starts the session using an open GET request over the HTTPS persistent connection.

The BlackBerry Collaboration Service receives events that the server initiates from the Microsoft Office Communicator Web Access server using an HTTP GET or HTTPS GET request, and sends the events to the collaboration client over the session. The BlackBerry Collaboration Service sends events that the BlackBerry device initiates to the Microsoft Office Communicator Web Access server using an HTTP POST or HTTPS POST request.

Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Communications Server 2007



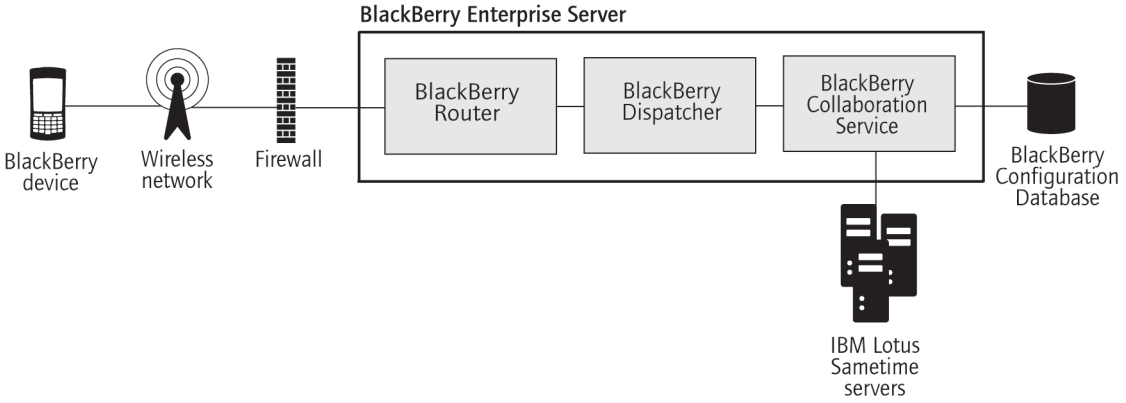
1. A user logs in to a collaboration client on a BlackBerry® device.
2. The BlackBerry device compresses and encrypts the user ID and password, and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion® proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
   - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on BlackBerry devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
   - If no idle sessions exist, the BlackBerry Collaboration Service sends a "Server Busy" status message to the BlackBerry device and rejects the login request.
   - If the maximum number of sessions is not set and the number of sessions equals the total number that the HTTP persistent connection supports, the BlackBerry Collaboration Service sends a "Failed" status message to the BlackBerry device and rejects the login request.

   The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and tries to authenticate the user using Integrated Windows® Authentication. If the authentication is not successful, the BlackBerry Collaboration Service tries a forms-based login process instead. The BlackBerry Collaboration Service sends a login request in XML format to the Microsoft® Office Communicator Web Access Server.

   The BlackBerry Collaboration Service opens the connection using HTTPS over port 443. You can also configure the connection to use HTTP, the transport protocol that the AJAX service uses, or a custom port number.
5. The Microsoft Office Communicator Web Access server formats the request using a Microsoft API and sends the request to the Microsoft® Office Live Communications Server over an MTLS connection.
6. The Microsoft Office Live Communications Server accepts the request, processes the login information, and sends the acceptance to the Microsoft Office Communicator Web Access server.
7. The Microsoft Office Communicator Web Access server sends the acceptance to the BlackBerry Collaboration Service.
8. The BlackBerry Collaboration Service sends the acceptance, in encrypted and compressed format, through the BlackBerry Dispatcher to the BlackBerry device, and creates a cache of the connectivity information to maintain the instant messaging session.
9. The collaboration client on the BlackBerry device starts the session using an open GET request over the HTTPS persistent connection.

The BlackBerry Collaboration Service receives events that the server initates from the Microsoft Office Communicator Web Access server using an HTTP GET or HTTPS GET request, and sends the events to the collaboration client over the session. The BlackBerry Collaboration Service sends events that the BlackBerry device initiates to the Microsoft Office Communicator Web Access server using an HTTP POST or HTTPS POST request.

Process flow: Starting an instant messaging session using the BlackBerry Client for IBM Lotus Sametime



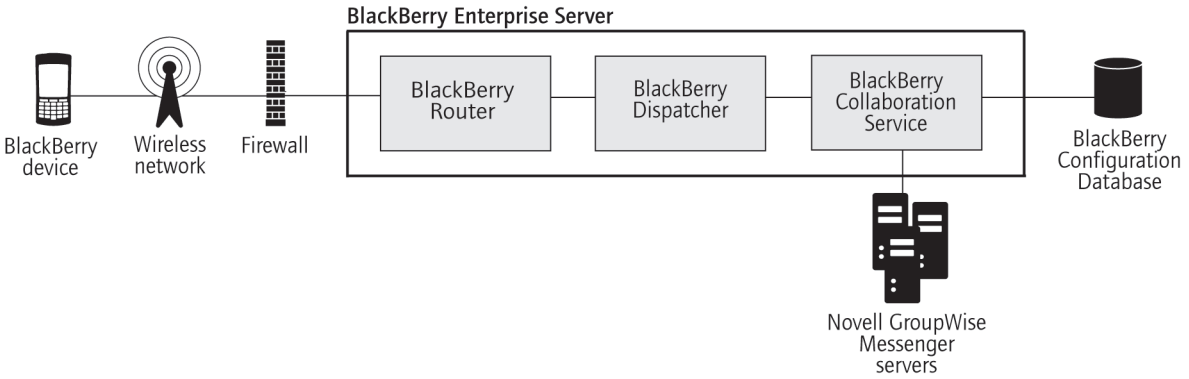
1. A user logs in to a collaboration client on a BlackBerry® device.
2. The BlackBerry device compresses and encrypts the user ID and password, and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion® proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
   - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on BlackBerry devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
   - If no idle sessions exist, the BlackBerry Configuration Database sends a "Server Busy" status message to the BlackBerry device and rejects the login request.
   - If the maximum number of sessions is not set and the number of sessions equals the total number that the IBM® Lotus® Sametime® API supports, the BlackBerry Configuration Database sends a "Failed" status message to the BlackBerry device and rejects the login request.

   The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and connects to the IBM Lotus Sametime server. The BlackBerry Collaboration Service starts an encrypted proxy connection over TCP/IP using the IBM Lotus Sametime API, reformats the request from the RIM proprietary protocol format into one that the IBM Lotus Sametime API supports, and sends the request.

   By default, the BlackBerry Collaboration Service starts the connection over port 1533 unless you specify a custom port number.

5. The IBM Lotus Sametime server accepts the login request from the BlackBerry device, starts a dedicated TCP/IP connection for the session, and listens for requests from the BlackBerry device for the session.
6. The BlackBerry Collaboration Service sends the acceptance, in encrypted and compressed format, through the BlackBerry Dispatcher to the BlackBerry device, and creates a cache of the connectivity information to maintain the instant messaging session.

Process flow: Starting an instant messaging session using the BlackBerry Client for Novell GroupWise Messenger



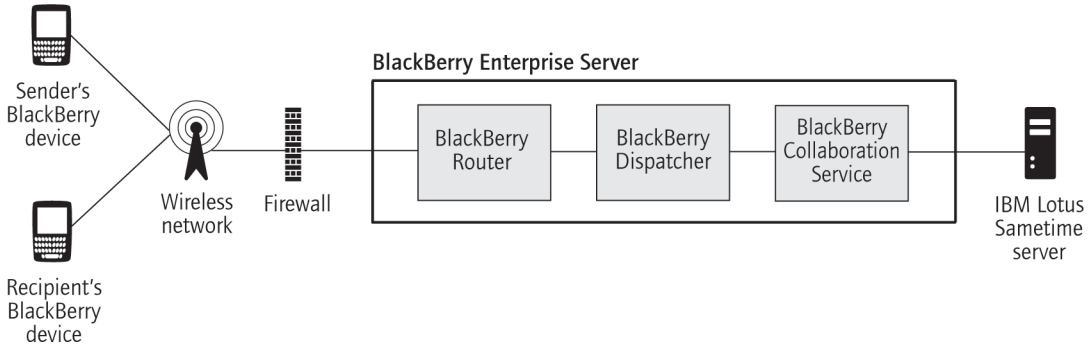
1. A user logs in to a collaboration client on a BlackBerry® device.
2. The BlackBerry device compresses and encrypts the user ID and password and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
   - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on BlackBerry devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
   - If there are no idle sessions, the BlackBerry Configuration Database sends a "Server Busy" status message to the BlackBerry device and rejects the login request.
   - If the maximum number of sessions is not set and the number of sessions equals the total number that the Novell® GroupWise® protocol supports, the BlackBerry device sends a "Failed (300)" status message to the BlackBerry device and rejects the login request.

The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and connects to the Novell GroupWise Messenger server.

The BlackBerry Collaboration Service starts an encrypted proxy (SSL) connection using the Novell GroupWise protocol and sends the request. By default, the BlackBerry Collaboration Service opens the connection over port 8300, but it can also open the connection over a custom port number.

5. The Novell GroupWise Messenger server accepts the login request from the BlackBerry device, opens a dedicated SSL connection for the session, and listens for requests from the BlackBerry device.
6. The BlackBerry Collaboration Service sends the acceptance, in encrypted and compressed format, through the BlackBerry Dispatcher to the BlackBerry device, and creates a cache of the connectivity information to maintain the instant messaging session.

Process flow: Sending a file to a contact using the BlackBerry Client for IBM Lotus Sametime



1. A user opens a conversation with a contact, clicks Send File on the menu, and selects a file to send to the contact.
2. The BlackBerry® Client for IBM® Lotus® Sametime® creates an invitation request and sends it to the BlackBerry Collaboration Service.
3. The BlackBerry Collaboration Service checks the size of the file to verify that it does not exceed the maximum file size that you configure on the BlackBerry® Enterprise Server, associates the file extension and the conversation ID with the invitation request, and sends the request to the IBM Lotus Sametime server.
4. The IBM Lotus Sametime server checks the file size to verify that it does not exceed the maximum file size that you configured on the IBM Lotus Sametime server (by default, 1 MB), associates the file with the conversation that is open between the sender and recipient, and sends the request to the BlackBerry Collaboration Service.
5. The BlackBerry Collaboration Service converts the request into an instant messaging invitation and sends it to the client on the recipient's BlackBerry device.
6. In the conversation window on the recipient's client, the recipient receives a request to accept or decline the file. The recipient can also select an option to optimize the file for viewing on the BlackBerry device.

The BlackBerry Collaboration Service can optimize files for viewing on the BlackBerry device only if it has access to the BlackBerry Attachment Service in your organization's environment.

7. The recipient accepts the request.

   If the recipient selected the optimize option, the file will be downloaded to the memory of the BlackBerry device. If the recipient did not select the optimize option, the client prompts the recipient to save the file to a location in the file system on the BlackBerry device.
8. The recipient's client sends a content request packet to the BlackBerry Collaboration Service.
9. The BlackBerry Collaboration Service requests the file size from the IBM Lotus Sametime server, and sends data to the IBM Lotus Sametime server to begin the file transfer process.

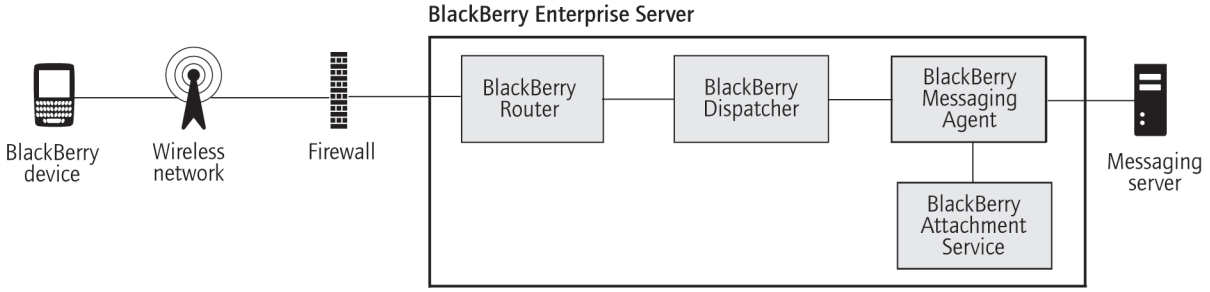
   By default, the media transfer state on the BlackBerry Collaboration Service is set to transfer.
10. The sender's client sends the data for the file in content message packets to the BlackBerry Collaboration Service.
11. The BlackBerry Collaboration Service checks the order of the content message packets and sends them to the recipient's client using a BlackBerry instant messaging protocol.
12. The recipient's client receives the first content message packet, sends an acknowledgement message to the BlackBerry Collaboration Service, and requests the next content message packet from the BlackBerry Collaboration Service. This continues until the client receives all of the content message packets.

    If the recipient selected the option to optimize the file for viewing, the BlackBerry Attachment Service converts the file into a format that is optimized for viewing on the BlackBerry device.
13. When the BlackBerry Collaboration Service receives an acknowledgement message for the last content message packet from the recipient's client, it changes its media transfer state to done and stops the file transfer process on the IBM Lotus Sametime server.
14. In the conversation window, the client notifies the recipient that the file has been received.

    The recipient can open the file from the conversation window or from the file system on the BlackBerry device. The BlackBerry device uses the BlackBerry® Browser to render supported files. If the recipient selected the option to optimize the file for viewing, the recipient can open and view supported files in the attachment viewer on the BlackBerry device. The recipient can also save the optimized file to a location in the file system on the BlackBerry device.

Message attachment process flows

Process flow: Viewing a message attachment



1. A user receives a message with an attachment on a BlackBerry® device.
2. The BlackBerry Messaging Agent verifies that the format of the attachment is valid for conversion.

   If the format is not valid and the user's BlackBerry device is Java® based, the Open Attachment menu item does not appear on the user's BlackBerry device.
3. The user clicks the Open Attachment menu item to view the attachment on the BlackBerry device.
4. The attachment viewer sends the request to the BlackBerry Messaging Agent.
5. The BlackBerry Messaging Agent connects to the BlackBerry Attachment Service over port 1900.
6. The BlackBerry Attachment Service retrieves the attachment in binary format from the user's message store using the BlackBerry Messaging Agent link to the messaging server.

   The BlackBerry Attachment Service distills the attachment and extracts the content, layout, appearance, and navigation information from the attachment.

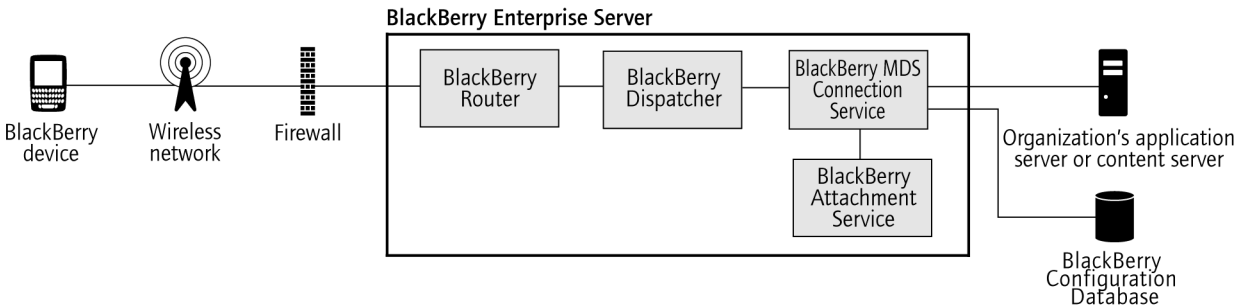
   The BlackBerry Attachment Service organizes, stores, and links the information in a proprietary DOM in a binary XML style.

   The BlackBerry Attachment Service formats the attachment for the BlackBerry device and converts it to UCS format. The formatting is based on the request for content (for example, page and paragraph information, or search words) and the available BlackBerry device information (for example, screen size, display, or available space).

   The BlackBerry Attachment Service sends the UCS data to the BlackBerry Messaging Agent using a TCP/IP connection over port 1900.
7. The BlackBerry Messaging Agent sends the converted attachment to the BlackBerry Dispatcher.
8. The BlackBerry Dispatcher compresses the first portion of the attachment, encrypts it using the master encryption key of the BlackBerry device, and sends the first portion of the attachment to the BlackBerry Router.

9. The BlackBerry Router sends the first portion of the attachment to the wireless network over port 3101.
10. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network.
11. The wireless network delivers the attachment to the BlackBerry device.
12. The BlackBerry device sends a delivery confirmation to the BlackBerry Dispatcher, which sends it to the BlackBerry Messaging Agent. If the BlackBerry® Enterprise Server does not receive a delivery confirmation within 4 hours, it sends the attachment data to the wireless network again.
13. The BlackBerry device uses its master encryption key to decrypt and decompress the attachment so that the user can view the attachment.
14. The user views the attachment on the BlackBerry device by selecting a section from the table of contents, or by viewing the full attachment. The original formatting of the attachment, including indents, tables, fonts, and bullets, is reflected on the BlackBerry device.

Process flow: Viewing an attachment using a link



1. A user clicks the Get Link menu item to view an attachment on a BlackBerry® device.
2. The BlackBerry device sends the request to the BlackBerry® Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service creates an HTTP session for the user and sends the request to the web server.

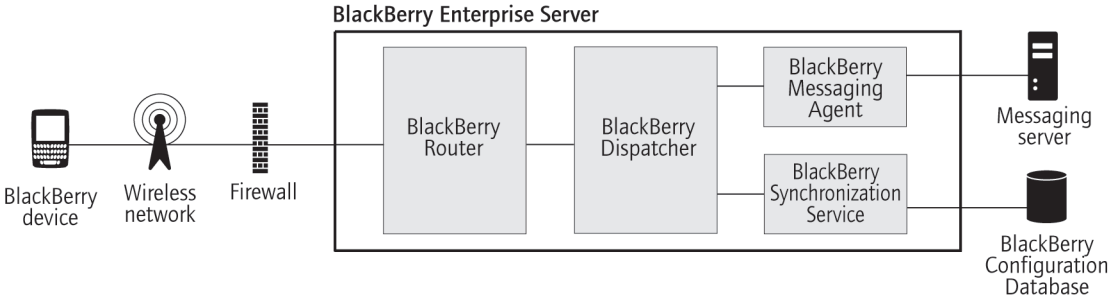
   The BlackBerry MDS Connection Service retrieves the requested content and sends it to the BlackBerry Attachment Service.
5. The BlackBerry Attachment Service extracts the content, layout, appearance, and navigation information from the attachment and organizes, stores, and links the information in a proprietary DOM in a binary XML style.
6. The BlackBerry Attachment Service formats the attachment for the BlackBerry device and converts it to UCS format.

   The formatting is based on the request for content (for example, page and paragraph information, or search words) and the available BlackBerry device information (for example, screen size, display, or available space).
7. The BlackBerry Attachment Service sends the converted attachment to the BlackBerry MDS Connection Service using HTTP.
8. The BlackBerry MDS Connection Service sends the first 250 KB of content to the BlackBerry Dispatcher over port 3200.

9. The BlackBerry Dispatcher compresses the content, encrypts it using the master encryption key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
10. The BlackBerry Router sends the encrypted content to the BlackBerry device.
11. The BlackBerry device uses its master encryption key to decrypt and decompress the attachment content so that the user can view the attachment.
12. The user views the attachment on the BlackBerry device using the browser plug-in for the attachment viewer. The attachment viewer processes 3 KB at a time.

Organizer data process flows

Process flow: Synchronizing organizer data for the first time on a BlackBerry device



1. A user activates a new BlackBerry® device or upgrades an existing BlackBerry device and receives the service book for the BlackBerry Synchronization Service.
2. The BlackBerry device requests the synchronization configuration information from the BlackBerry Synchronization Service.

   The configuration information indicates whether wireless data synchronization on the BlackBerry® Enterprise Server is turned on, and which database can be synchronized. The configuration information also provides database synchronization types and conflict resolution settings. All data that the BlackBerry device and BlackBerry Enterprise Server send between each other is compressed and encrypted.
3. The BlackBerry Synchronization Service returns the configuration information and synchronizes the databases using that information.

   A synchronization agent on the BlackBerry device tracks which databases can be synchronized over the wireless network. If data already exists on both the BlackBerry device and BlackBerry Enterprise Server, the BlackBerry Synchronization Service merges, adds, or updates the records during the synchronization process. If data exists on only the BlackBerry device or BlackBerry Enterprise Server, the BlackBerry Synchronization Service restores the data from the appropriate location. The BlackBerry device and BlackBerry Enterprise Server do not delete records during the initial synchronization process.

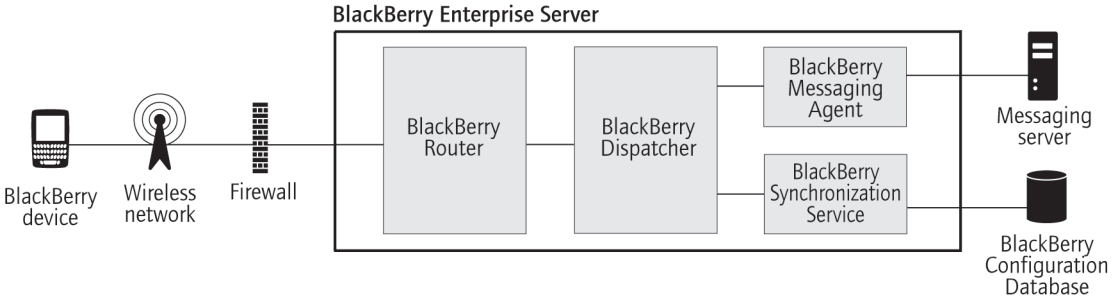
After the BlackBerry Synchronization Service registers a database for wireless data synchronization, it can no longer be synchronized or restored using the BlackBerry® Desktop Software.

The initial synchronization process is complete when the data on the BlackBerry device and the data on the BlackBerry Enterprise Server are synchronized. Future changes on the BlackBerry device or BlackBerry Enterprise Server are synchronized over the wireless network.

If the user changes data on the BlackBerry device or in the organizer application on the user's computer during the initial synchronization process, the BlackBerry Synchronization Service synchronizes the changes after the initial synchronization completes.

If the user connects the BlackBerry device to a computer that is running the BlackBerry® Device Manager, the initial synchronization process can occur over the connection to the BlackBerry Router instead of over the wireless network.

Process flow: Synchronizing subsequent changes to organizer data



1. A user saves a change to the organizer data or BlackBerry® device settings (for example, a new AutoText entry) on a BlackBerry device or in the organizer application on the user's computer.
2. Depending on where the user made the change, the BlackBerry device or the BlackBerry® Enterprise Server adds the change to a changelist and sends the changelist to the BlackBerry Synchronization Service.

   The changelist includes the target database and record information for the organizer application.
3. The BlackBerry Synchronization Service sends a change to organizer data over the wireless network, along with other entries in the changelist for the user.

   The BlackBerry Synchronization Service sends other changes, including BlackBerry device information, time zone information, and backup and restore data, at the batch synchronization interval that is set on the BlackBerry Enterprise Server. By default, the batch synchronization interval is 10 minutes.

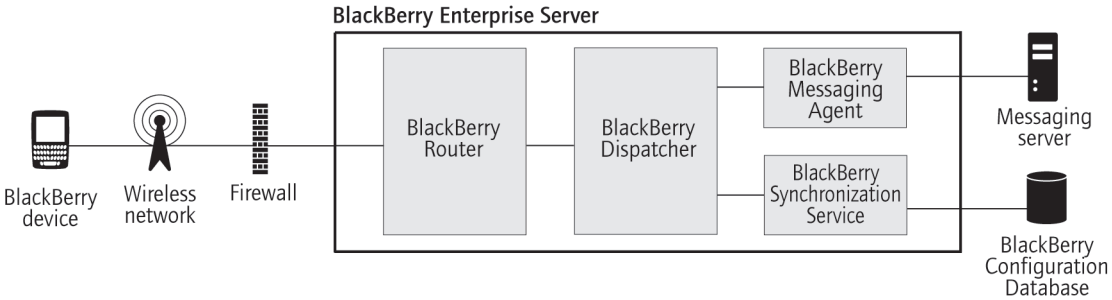
   To prevent synchronization errors, the BlackBerry Enterprise Server and BlackBerry device can send only a single changelist at a time for a user account.

The BlackBerry Synchronization Service writes a synchronization request entry to the SynchRequest table of the BlackBerry Configuration Database, and sends the changed records to the BlackBerry Dispatcher.

4. The BlackBerry Dispatcher compresses the content, encrypts it using the master encryption key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router for delivery to the BlackBerry device.
5. The BlackBerry device sends a delivery confirmation to the BlackBerry Synchronization Service for each record that it receives.
6. The BlackBerry Synchronization Service receives delivery confirmations, deletes the corresponding synchronization request entries from the SyncRequest table, and writes an entry to the SyncRecordState table for each delivery confirmation.

Each organizer database record has a unique identifier that is mapped to a corresponding record on the BlackBerry device.

Process flow: Adding a contact picture on a BlackBerry device



1. A user adds a picture to a contact in the address book on a BlackBerry® device and saves the change.
2. The BlackBerry device creates a changelist request to synchronize the changed record. The changelist request includes the updated record information and identifies the address book as the target for the update.

   The BlackBerry device compresses and encrypts the request, and sends the request to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher uses the master encryption key of the BlackBerry device to decrypt and decompress the request, and sends the request to the BlackBerry Synchronization Service.
4. The BlackBerry Synchronization Service receives the changelist request, writes a synchronization request entry in the SynchRequest table of the BlackBerry Configuration Database, and sends the changed record to the BlackBerry Dispatcher.
5. The BlackBerry Dispatcher sends the changed record, in XML format, to the BlackBerry Messaging Agent.

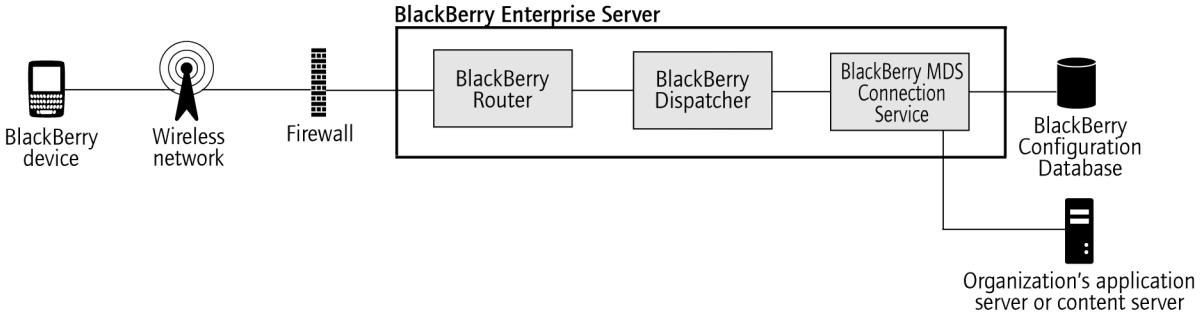
   If the file size of the picture exceeds 32 KB, the BlackBerry Messaging Agent rejects the synchronization request.
6. The BlackBerry Messaging Agent sends the changed record to the messaging server.
7. The messaging server updates the user's personal contact list.
8. The BlackBerry Messaging Agent sends a delivery confirmation to the BlackBerry Dispatcher.
9. The BlackBerry Dispatcher sends the delivery confirmation to the BlackBerry Synchronization Service.

10. The BlackBerry Synchronization Service deletes the synchronization request entry from the SyncRequest table, writes an entry in the SyncRecordState table, and sends the delivery confirmation to the BlackBerry Dispatcher.
11. The BlackBerry Dispatcher encrypts the results using the master encryption key of the BlackBerry device, compresses them, and sends them to the BlackBerry Router.
12. The BlackBerry Router sends the results to the wireless network over port 3101.
13. The wireless network verifies that the PIN belongs to a valid BlackBerry device and sends the delivery confirmation to the BlackBerry device.

    If the BlackBerry device does not receive the delivery confirmation from the wireless network within 20 minutes, it sends the synchronization request to the wireless network again. If the BlackBerry device does not receive the delivery confirmation within 8 hours, it stops resending the synchronization request to the wireless network.

Mobile data process flows

Process flow: Requesting BlackBerry Browser content on a BlackBerry device



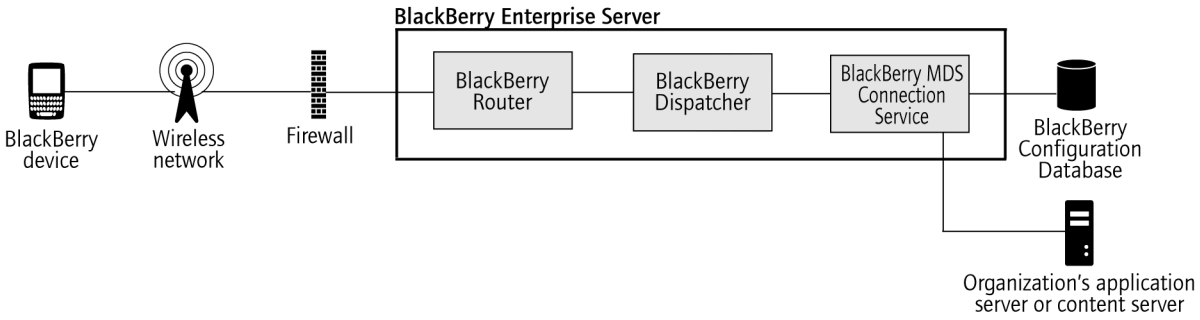
1. A user requests Internet or intranet content from your organization's content server using the BlackBerry® Browser on a BlackBerry device.
2. The BlackBerry device sends the request to the BlackBerry® Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service creates an HTTP session for the user and retrieves the requested Internet or intranet content from the content server.

   The BlackBerry MDS Connection Service converts the content so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.
5. The BlackBerry Dispatcher compresses the content, encrypts it using the master encryption key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.

6. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.
7. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network and sends the encrypted content to the BlackBerry device.
8. The BlackBerry device sends a delivery confirmation to the BlackBerry Router, and decrypts and decompresses the content so that the user can view it in the BlackBerry Browser.

   If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.

Process flow: Requesting BlackBerry Browser content while access control is turned on for the BlackBerry MDS Connection Service



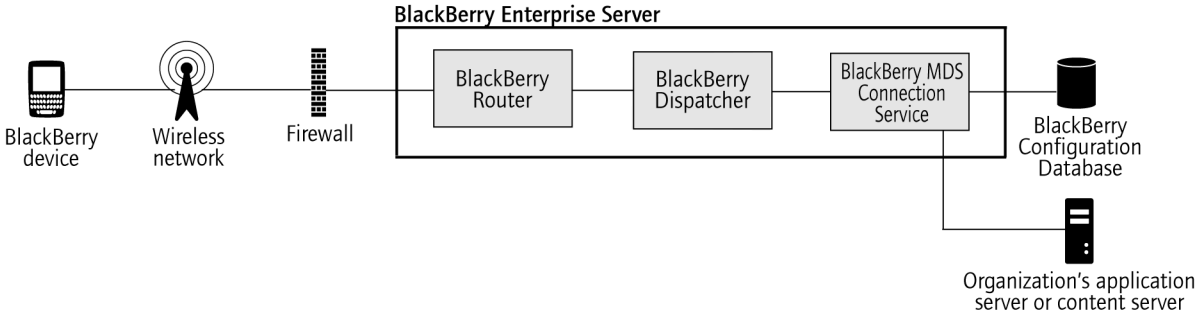
1. A user requests Internet or intranet content from your organization's content server using the BlackBerry® Browser on a BlackBerry device.
2. The BlackBerry device sends the request to the BlackBerry® Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service checks the BlackBerry Configuration Database to verify whether pull authorization is turned on, and whether the user has permission to pull content from the specified content server.

   If the user does not have permission to pull content from the specified content server, the BlackBerry MDS Connection Service rejects the request and sends an error message to the BlackBerry device.
5. The BlackBerry MDS Connection Service creates an HTTP session for the user and sends the user's authentication credentials to the content server. If the user authenticates, the BlackBerry MDS Connection Service sends the HTTP request to the content server. If the user does not authenticate, the BlackBerry Browser displays an "HTTP 403 Error" message, and prompts the user to type the correct credentials.
6. The BlackBerry MDS Connection Service retrieves the content from the content server, converts it so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.

7. The BlackBerry Dispatcher compresses the content, encrypts it using the master encryption key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
8. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.
9. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network and sends the encrypted content to the BlackBerry device.
10. The BlackBerry device sends a delivery confirmation to the BlackBerry Router, and decrypts and decompresses the content so that the user can view it in the BlackBerry Browser.

    If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.

Process flow: Requesting BlackBerry Browser content with two-factor authentication turned on



1. A user requests Internet or intranet content from your organization's content server using the BlackBerry® Browser on a BlackBerry device.
2. The BlackBerry device sends the request to the BlackBerry® Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service checks whether the user's BlackBerry device is running an authenticated connection that can support the content request.

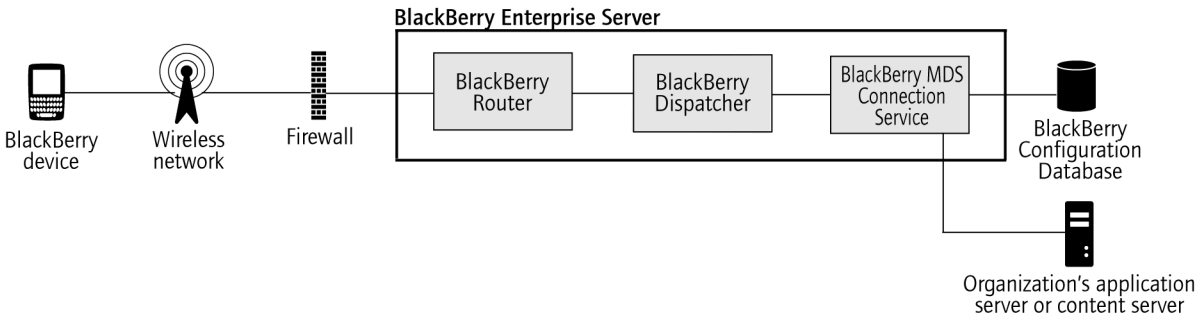
   If the BlackBerry device is not running an authenticated connection, the BlackBerry MDS Connection Service redirects the user to a login web page. If the user logs in, using an RSA SecurID® user name and passcode, the BlackBerry MDS Connection Service creates a connection to the content server. By default, the BlackBerry device caches the user's information for 24 hours of activity on the authenticated connection, or 60 minutes of inactivity.

   The BlackBerry MDS Connection Service creates an HTTP session for the user and retrieves the Internet or intranet content from the content server. The BlackBerry MDS Connection Service converts the content so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.

5. The BlackBerry Dispatcher compresses the content, encrypts it using the master encryption key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
6. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.
7. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network and sends the encrypted content to the BlackBerry device.
8. The BlackBerry device sends a delivery confirmation to the BlackBerry Router, and decrypts and decompresses the content so that the user can view it in the BlackBerry Browser.

   If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.

Process flow: Pushing application content to a BlackBerry device



1. A push application on an application server or a content server behind your organization's firewall sends an HTTP POST request to a central push server over the listen port for the content server. The default port number is 8080.

   You can define one or more instances of the BlackBerry® MDS Connection Service in a BlackBerry Domain as a central push server. A push application specifies the BlackBerry® Enterprise Server host name and the connection port number that the BlackBerry MDS Connection Service listens on.
2. The central push server checks the BlackBerry Configuration Database for the following information about the intended recipients of the application content: the PINs that are associated with the user accounts, whether the PINs are enabled for the BlackBerry MDS Connection Service, and the active BlackBerry Enterprise Server instances that the users are located on.

   User accounts that do not appear in the BlackBerry Configuration Database, or that are pending deletion, cannot receive the push content.

   The central push server responds to the push application to acknowledge that it is processing the request, and sends the push content to the BlackBerry MDS Connection Service instances that have active, primary connections to the BlackBerry Enterprise Server instances.

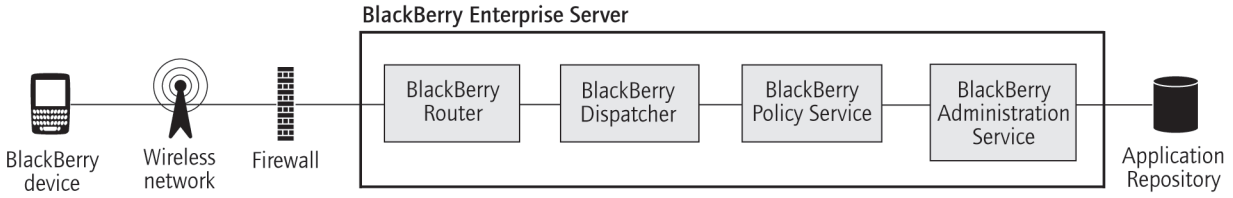
3. The BlackBerry MDS Connection Service converts the content so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.
4. The BlackBerry Dispatcher compresses the content, encrypts it using the master encryption key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
5. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.

   The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network, and sends the encrypted content to the BlackBerry device.
6. The BlackBerry device sends a delivery confirmation to the BlackBerry Router.

   If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.
7. The BlackBerry device decrypts and decompresses the content.

   The BlackBerry Application detects the incoming content by listening on a port number that the application developer specified. For example, the BlackBerry® Browser listens for push application connections on port 7874. The application displays the content on the BlackBerry device when the user runs the application.

Process flow: Installing a BlackBerry Java Application on a BlackBerry device over the wireless network



1. A developer creates a BlackBerry® Java® Application using the BlackBerry® Java® Development Environment or another Java authoring tool. The developer produces an application bundle.

   The application bundle contains an .alx file that stores information about the attributes of the BlackBerry Java Application, including the author name, a description of the application, and copyright information.
2. In the BlackBerry Administration Service, you publish the application bundle to the application repository.
3. You create a software configuration and add the BlackBerry Java Application to the software configuration. You specify that the application is required, assign an application control policy to the application, and specify wireless delivery to BlackBerry devices.

   You assign the software configuration to a group.

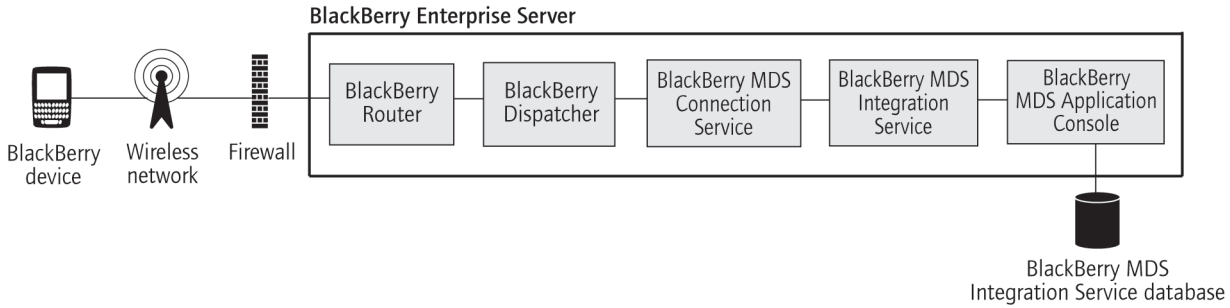
4. The BlackBerry Administration Service creates a deployment job.

   A deployment job represents the objects that must be sent to each user's BlackBerry device and consists of multiple tasks. Each task manages the delivery of an object (for example, a BlackBerry Java Application, an access control policy, or an IT policy) to a BlackBerry device.
5. The delivery manager component of the BlackBerry Administration Service receives tasks to send a BlackBerry Java Application to BlackBerry devices.
6. The BlackBerry Administration Service exports the files for the BlackBerry Java Application to a shared network folder.
7. The delivery manager converts the tasks into send module commands, queues send module commands into logical groups for each user, and sends the send module commands to the BlackBerry Policy Service. Separate applications are queued in separate groups.
8. The BlackBerry Policy Service processes the send module commands in the queue in sequence. When the BlackBerry Policy Service processes a group of send module commands, it retrieves the data for the BlackBerry Java Application from the shared network folder, and sends the send module commands with the application data to the BlackBerry Dispatcher.

   If the send module commands are less than 56 KB, the BlackBerry Policy Service sends them in one data packet. If the send module commands exceed 56 KB, the BlackBerry Policy Service sends them in multiple data packets.
9. The BlackBerry Dispatcher sends the send module commands to the BlackBerry Router.
10. The BlackBerry Router sends the send module commands to a BlackBerry device over the wireless network.
11. The BlackBerry device installs the BlackBerry Java Application. The BlackBerry device sends an acknowledgement packet for the BlackBerry Java Application to the BlackBerry Router.
12. The BlackBerry Router sends the acknowledgement packet to the BlackBerry Dispatcher.
13. The BlackBerry Dispatcher delivers the acknowledgement packet to the BlackBerry Policy Service.
14. The BlackBerry Policy Service clears the send module commands for the BlackBerry device from the queue and processes the next group of send module commands that are in the queue.
15. The BlackBerry Administration Service displays that the BlackBerry Java Application was delivered to the BlackBerry device.

If the BlackBerry device does not receive all of the send module commands within 4 hours, the BlackBerry device sends a failure acknowledgement packet to the BlackBerry Policy Service. The BlackBerry Administration Service detects the failure acknowledgement packet and displays an installation failure message for the BlackBerry device.

Process flow: Installing a BlackBerry MDS Runtime Application on a BlackBerry device over the wireless network



1. A developer creates a BlackBerry® MDS Runtime Application using the latest version of BlackBerry® MDS Studio or the BlackBerry® Plug-in for Microsoft® Visual Studio®. The developer produces an application bundle and publishes it to the BlackBerry MDS Application Repository.
2. The BlackBerry MDS Application Console displays the application as available for installation in the application directory view.
3. Using the BlackBerry MDS Application Console, you assign the BlackBerry MDS Runtime Application to the members of a group.
4. The BlackBerry MDS Application Console sends an installation request to the BlackBerry MDS Integration Service that you assign BlackBerry devices to.
5. The BlackBerry MDS Integration Service retrieves the files for the BlackBerry MDS Runtime Application from the BlackBerry MDS Application Repository. The BlackBerry MDS Integration Service repackages the files so that they can be sent to the BlackBerry device over the wireless network, and sends an installation request to the BlackBerry MDS Connection Service using the Push Access Protocol.
6. The BlackBerry MDS Connection Service sends the installation request to the BlackBerry Dispatcher.
7. The BlackBerry Dispatcher sends the installation request to the BlackBerry Router.
8. The BlackBerry Router sends the installation request to the BlackBerry device over the wireless network.
9. The BlackBerry device receives the installation request on the port number that the BlackBerry MDS Runtime uses to listen for incoming messages from the BlackBerry MDS Integration Service.

   If the BlackBerry device does not receive the installation request (for example, if the BlackBerry device is outside of a wireless coverage area), the BlackBerry MDS Integration Service tries to send the request up to two more times before it sends an installation failure message to the BlackBerry MDS Application Console.
10. The BlackBerry MDS Runtime on the BlackBerry device verifies that the BlackBerry MDS Runtime Application can be installed on the BlackBerry device.

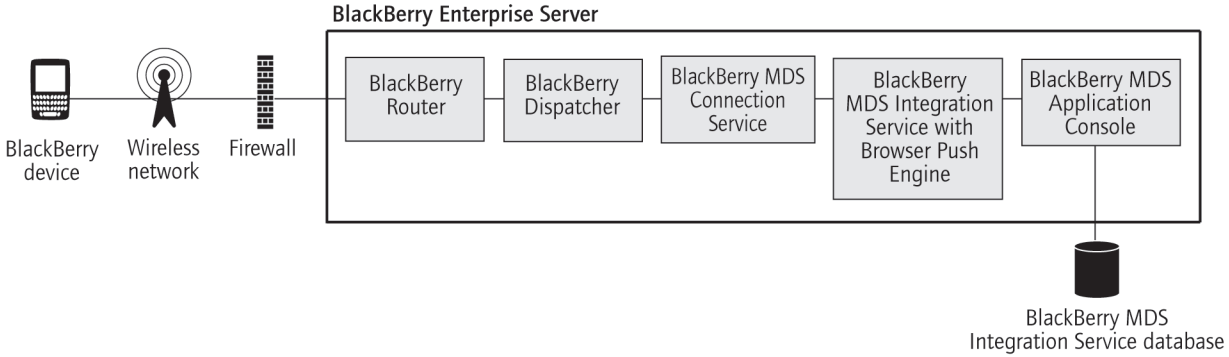
The BlackBerry MDS Runtime sends a confirmation message to the BlackBerry MDS Integration Service and retrieves the files that are required to install the BlackBerry MDS Runtime Application. The BlackBerry MDS Integration Service sends other information about the application to the BlackBerry device, including identification information, signing information, and the URI version.

The BlackBerry MDS Runtime installs the BlackBerry MDS Runtime Application on the BlackBerry device and sends a delivery confirmation message to the BlackBerry MDS Integration Service.

If the BlackBerry MDS Runtime cannot install the BlackBerry MDS Runtime Application on the BlackBerry device, it sends an installation failure message to the BlackBerry MDS Integration Service, which sends the message to the BlackBerry MDS Application Console.

11. The BlackBerry MDS Integration Service reports the status of the installation to the BlackBerry MDS Application Console.
12. The BlackBerry MDS Application Console displays that the BlackBerry MDS Runtime Application is installed on the BlackBerry device.

Process flow: Installing a BlackBerry Browser Application on a BlackBerry device over the wireless network



1. A developer creates a BlackBerry® Browser Application using a template. The developer produces an application bundle that contains two .xml files.

   The ApplicationAttributes.xml file contains application attributes. The deployment .xml file contains deployment information and specifies the web address to push to and display on BlackBerry devices.
2. Using the BlackBerry MDS Application Console, you publish the application bundle to the BlackBerry MDS Application Repository.

   Using the BlackBerry MDS Application Console, you assign a BlackBerry Browser Application to a group.
3. The BlackBerry MDS Application Console sends an installation message to the BlackBerry MDS Integration Service that BlackBerry devices are assigned to.

4. The Browser Push Engine on the BlackBerry MDS Integration Service sends the installation message to the BlackBerry MDS Connection Service using Push Access Protocol.
5. The BlackBerry MDS Connection Service sends the installation message to the BlackBerry Dispatcher.
6. The BlackBerry Dispatcher sends the installation message to the BlackBerry Router.
7. The BlackBerry Router sends the installation message to a BlackBerry device over the wireless network.

   The BlackBerry device receives the installation message on the port number that it uses to listen for browser updates.
8. The BlackBerry Browser Application installs on the BlackBerry device. Depending on the type of BlackBerry Browser Application, one of the following occurs on the BlackBerry device:
   - If the application is a browser channel push application, an "unread" icon displays on the Home screen of the BlackBerry device. After the user clicks the icon to view the web page in the BlackBerry® Browser, the icon becomes a "read" icon.
   - If the application is a browser cache push application, the web page is stored in the cache of the BlackBerry Browser. To access the web page, the user can browse to the web address using the BlackBerry Browser.
   - If the application is a browser message push application, an email message that includes the web address appears in the message list.

The Browser Push Engine on the BlackBerry MDS Integration Service polls the web page that is specified in the BlackBerry Browser Application for changes. The configuration that is specified in the deployment .xml file specifies the frequency of the polling interval. When the Browser Push Engine detects changes to the web page, it pushes a browser update to the BlackBerry device. Depending on the type of BlackBerry Browser Application, the updated web page is displayed through an "unread" icon on the home screen, updated in the BlackBerry Browser cache, or linked to a new message in the messages list on the BlackBerry device.

BlackBerry device management process flows

Process flow: Activating a BlackBerry device over the wireless network

A user receives or purchases a new BlackBerry® device.

1. The user contacts your organization's IT department to activate the BlackBerry device.
2. You create a temporary activation password for the user account and communicate the password to the user. The password applies to the user account only.
3. To activate the BlackBerry device over the wireless network, the user opens the activation application on the BlackBerry device and types the appropriate email address and activation password.
4. The BlackBerry device sends an activation request message to the email account. The message contains information about the BlackBerry device, such as routing information and the public keys for the BlackBerry device.
5. The BlackBerry® Enterprise Server sends the BlackBerry device an activation response that contains routing information about the BlackBerry Enterprise Server and the public keys for the BlackBerry Enterprise Server.

The BlackBerry Enterprise Server and BlackBerry device establish a master encryption key. The BlackBerry Enterprise Server and BlackBerry device confirm knowledge of the master encryption key to each other. If the confirmation is successful, the activation proceeds and further communication between the BlackBerry Enterprise Server and BlackBerry device is encrypted.

The BlackBerry Enterprise Server sends the IT policy to the BlackBerry device. If the BlackBerry device cannot accept the IT policy, the activation process does not complete.

The BlackBerry Enterprise Server sends the appropriate service books (for example, the messaging service book, wireless calendar service book, browser service book, and other service books) to the BlackBerry device. The user can now send messages from and receive messages on the BlackBerry device.

6. If the user account is configured for wireless synchronization, and if wireless backup and wireless calendar synchronization on the BlackBerry device are turned on, the BlackBerry Enterprise Server sends user data to the BlackBerry device.

Process flow: Resending an IT policy to a BlackBerry device manually

1. Click a user account, and then click **Resend IT Policy**.
2. The BlackBerry Policy Service reads the current IT policy settings for the user account from the BlackBerry Configuration Database to determine which IT policy to send to the BlackBerry device.

   The BlackBerry Policy Service prepares to send the IT policy using the GME protocol by adding the unique identifier and BlackBerry® Enterprise Server version.

   The BlackBerry Policy Service adds the unique key that the BlackBerry Domain uses to sign IT policy data packets to the IT policy data packet.

   The BlackBerry Policy Service sends the IT policy data packet to the BlackBerry Dispatcher.
3. The BlackBerry Dispatcher encrypts the IT policy data packet using the master encryption key of the BlackBerry device, compresses the content, and sends it to the BlackBerry Router for delivery to the BlackBerry device.
4. The BlackBerry Router sends the encrypted IT policy data packet to the wireless network over port 3101. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network.

Process flow: Authenticating data on a BlackBerry device without connecting to the BlackBerry Infrastructure

1. A user connects a BlackBerry® device to a computer that the BlackBerry® Device Manager is running on.
2. The BlackBerry Router uses a unique authentication protocol to verify that the user is a valid BlackBerry device user.

   The authentication sequence uses the same authentication information for the BlackBerry® Enterprise Server and BlackBerry device that the SRP authentication sequence uses to validate the BlackBerry Enterprise Server before permitting it to connect to the BlackBerry® Infrastructure. The BlackBerry Router cannot access the value of the master encryption key of the BlackBerry device and BlackBerry Enterprise Server.

3. The BlackBerry device and BlackBerry Router use the BlackBerry Device Manager to send data to each other over the physical connection, behind the firewall. All the data that the BlackBerry device and BlackBerry Enterprise Server send to each other is compressed and encrypted. This data bypasses the wireless network.

   The transfer of wireless data over an SRP connection is restored when the user disconnects the BlackBerry device from the computer or closes the BlackBerry Device Manager.

Monitoring process flows

Process flow: Updating and displaying data in the BlackBerry Monitoring Service console

1. The BlackBerry® Monitoring Service Polling Engine polls all BlackBerry® Enterprise Server components for SNMP data about BlackBerry Enterprise Server components and BlackBerry device users. The BlackBerry Monitoring Service Polling Engine sends the SNMP data to the BlackBerry Monitoring Service Application Core.
2. The BlackBerry Monitoring Service Application Core processes the SNMP data and updates the data in the BlackBerry Monitoring Service console by performing the following actions:
   - updates statistics for data attributes of BlackBerry Enterprise Server components and BlackBerry device users
   - updates the alarm state for data attributes
   - generates notification messages for any data attributes with an alarm state that is changing
3. The BlackBerry Monitoring Service console displays the updated data.

Process flow: Storing data in the BlackBerry Monitoring Service database

1. The BlackBerry® Monitoring Service Polling Engine polls all BlackBerry® Enterprise Server components for SNMP data and sends the data to the BlackBerry Monitoring Service Data Collection Subsystem.
2. The BlackBerry Monitoring Service Data Collection Subsystem processes the SNMP data and sends the data to the BlackBerry Monitoring Service database.
3. The BlackBerry Monitoring Service database stores the data.

Wi-Fi enabled BlackBerry devices

6

Wi-Fi® enabled BlackBerry® devices permit users with qualifying data plans to access BlackBerry services over a mobile network, Wi-Fi network, or both networks simultaneously.

When users can access a mobile network and a Wi-Fi network simulaneously, users can perform multiple tasks over both networks. For example, a user with a BlackBerry® 8820 smartphone can send messages over a Wi-Fi network and can make a call over the mobile network at the same time.

If users' mobile network providers make UMA technology (GAN technology) available, and users have subscribed to the UMA feature, Wi-Fi enabled BlackBerry devices can access the mobile network providers' voice and data services over a mobile network or over a Wi-Fi connection.

Wi-Fi enabled BlackBerry devices can open a Wi-Fi connection from an enterprise Wi-Fi network or, with a VPN session, from a home Wi-Fi network or Wi-Fi hotspot to connect directly to the BlackBerry Router.

Wi-Fi enabled BlackBerry devices are designed to open a connection to the BlackBerry® Internet Service, BlackBerry MDS Connection Service, BlackBerry® Messenger, and other BlackBerry devices for PIN messaging. You can verify with your organization's wireless service provider whether your organization's service plan provides access to these services over a Wi-Fi connection.

Types of Wi-Fi networks

Wi-Fi® enabled BlackBerry® devices can access BlackBerry services using enterprise Wi-Fi networks, home Wi-Fi networks, or hotspots.

Type	Description
enterprise Wi-Fi networks	An enterprise Wi-Fi network has multiple wireless access points to provide ubiquitous, hotspot, or ubiquitous and hotspot coverage. You can use a Wi-Fi enabled BlackBerry device in any coverage area. An enterprise Wi-Fi network can require strong authentication and link layer security. An organization might consider an enterprise Wi-Fi network to be untrusted and require that all Wi-Fi connections to the organization's network occur through a VPN concentrator. You must configure Wi-Fi enabled BlackBerry devices to support the authentication type that your organization uses. An enterprise Wi-Fi network permits optimized access to the BlackBerry® Enterprise Server over a direct IP connection to the BlackBerry Router.

Type	Description
home Wi-Fi networks	A home Wi-Fi network uses a single wireless access point to provide Internet access through a broadband gateway. The broadband gateway can implement NAT and enable VPN connections to traverse the firewall. You can configure a home Wi-Fi network with link layer security and password-based authentication. You must configure BlackBerry devices to support the authentication that the home Wi-Fi network requires. A home Wi-Fi network permits users to access all BlackBerry services from their Wi-Fi enabled BlackBerry devices using the BlackBerry® Infrastructure.
hotspots	A hotspot offered by an ISP, a mobile network provider, or a property owner can provide a Wi-Fi connection in public and semipublic areas. The network can be an open network without link layer encryption, with a captive portal for authentication. The captive portal blocks all network traffic except traffic that uses HTTP and it redirects HTTP requests to a login page. After a user logs in, the captive portal permits the user to access wireless network services. Hotspots can have a firewall, and they can permit VPN connections. A hotspot enables users to access all BlackBerry services from their Wi-Fi enabled BlackBerry devices using the BlackBerry Infrastructure.

Wireless access points

Wi-Fi® enabled BlackBerry® devices use wireless access points to connect to the Wi-Fi network. An access point must conform to the IEEE® 802.11a, IEEE 802.11b, or IEEE 802.11g wireless networking standard.

Type	Description
thin access point	A thin access point (or controller-based access point) is part of an enterprise Wi-Fi network that you can manage from a central location. This type of access point requires an external controller to manage network traffic. You can administer one or more thin access points through the controller.

Type	Description
	Thin access points with an external controller can provide a more seamless roaming experience for users with Wi-Fi enabled BlackBerry devices during data and voice sessions.
thick access point	A thick access point (or intelligent or autonomous access point), has the intelligence to operate as a standalone component without a controller.

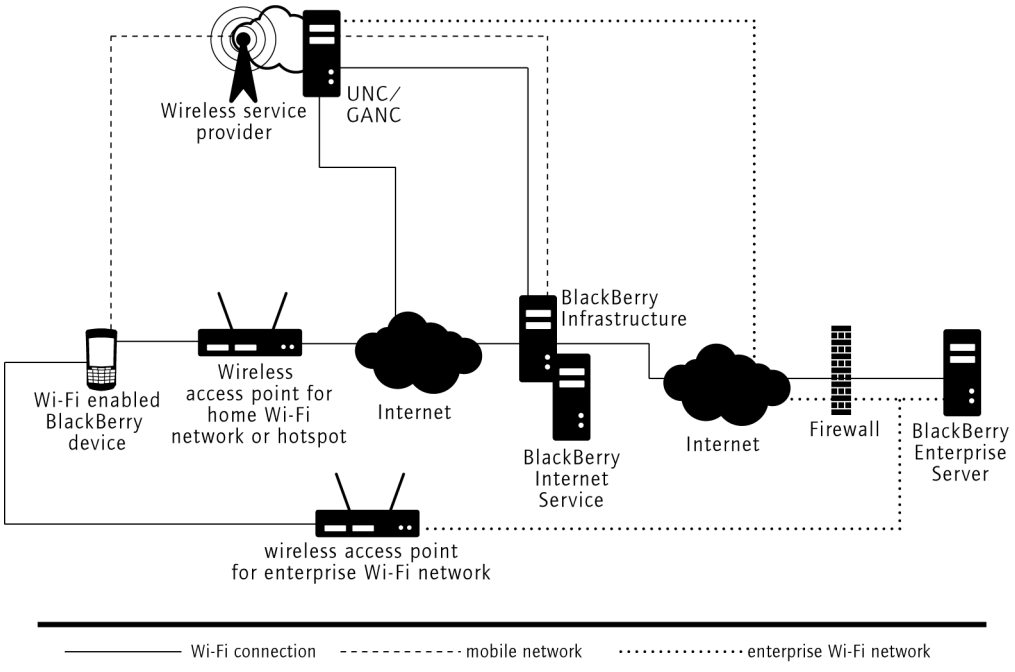
BlackBerry Enterprise Server support for Wi-Fi enabled BlackBerry devices

Feature	Description
activation of BlackBerry® devices over an enterprise Wi-Fi® network	Activation of BlackBerry devices over an enterprise Wi-Fi network is designed to simplify the activation or updating of BlackBerry devices.
connection to the BlackBerry Router	A connection to the BlackBerry Router is required for a Wi-Fi enabled BlackBerry device to connect to the BlackBerry® Enterprise Server over a Wi-Fi network to access your organization's data. If you do not use layer 2 or layer 3 access security, you can help to protect access to your organization's trusted LAN by installing the BlackBerry Router component in the DMZ, outside your organization's firewall. You can also enable access to the enterprise Wi-Fi network using a captive portal.
Direct access to the BlackBerry® Infrastructure over a Wi-Fi connection	Direct access to the BlackBerry Infrastructure over a Wi-Fi connection means that Wi-Fi enabled BlackBerry devices can access BlackBerry services over the Internet, even if UMA is not available. You can verify with your organization's wireless service provider that your organization's service plan supports access to BlackBerry messaging services over a Wi-Fi connection.
expanded groups of Wi-Fi and VPN configuration settings	Expanded groups of Wi-Fi and VPN configuration settings provide the ability to control Wi-Fi connections from BlackBerry devices.
multiple Wi-Fi and VPN profiles	Multiple Wi-Fi and VPN profiles are designed to address user needs in a variety of environments.
software token provisioning	Software token provisioning is designed to permit you to centrally provision and manage the seed for software token authentication (for example, for VPN connections) on BlackBerry devices.

Feature	Description
	The BlackBerry Enterprise Server is designed to work with the RSA® Authentication Manager to provide software token support for use with layer 2 and layer 3 authentication on supported BlackBerry devices.
user-specific configuration settings and IT policy rules	User-specific configuration settings and IT policy rules are designed to simplify the configuration of user-specific Wi-Fi and VPN information (such as user IDs and passwords).
wireless backup of Wi-Fi and VPN profiles	Wireless backup of Wi-Fi and VPN profiles on BlackBerry devices over a Wi-Fi connection enables users to restore the profiles, if necessary.
wireless software updates	Wireless software updates allow users to update the BlackBerry® Device Software without using the BlackBerry® Desktop Manager or first downloading the software update to a computer.

Connections that BlackBerry devices make to mobile and Wi-Fi networks

Wi-Fi® enabled BlackBerry® devices connect to different components in the the mobile and Wi-Fi networks so that they can communicate with the BlackBerry® Enterprise Server and provide BlackBerry services for users.



Component	Description
BlackBerry Enterprise Server	The BlackBerry Enterprise Server provides productivity tools and data from an organization's applications to BlackBerry devices over the wireless network, and processes, routes, compresses, and encrypts data.
BlackBerry® Infrastructure	The BlackBerry Infrastructure is designed to communicate with the BlackBerry Enterprise Server using a RIM proprietary protocol SRP.
BlackBerry® Internet Service	The BlackBerry Internet Service is an email and Internet service for BlackBerry devices that is designed to provide subscribers with automatic delivery of email messages, mobile access to email message attachments, and convenient access to Internet content.
UNC/GANC	The UNC/GANC is the gateway for Wi-Fi or mobile communications. The UNC/GANC exists in your organization’s gateway only if the wireless service provider supports UMA.
wireless access point for a home Wi-Fi network or hotspot	An access point for a home Wi-Fi network or hotspot permits the BlackBerry device to connect to a home Wi-Fi network or hotspot.
wireless access point for an enterprise Wi-Fi network	An access point for an enterprise Wi-Fi network permits a BlackBerry device to connect to an enterprise Wi-Fi network using strong authentication and link layer security.

Component	Description
wireless service provider	A wireless service provider is a telephone company that provides services for BlackBerry devices.
Wi-Fi enabled BlackBerry device	A Wi-Fi enabled BlackBerry device permits a user to access voice and data services across multiple radio technologies.

Connecting Wi-Fi enabled BlackBerry devices to the BlackBerry Enterprise Server over a Wi-Fi connection

Direct connections between BlackBerry devices and the BlackBerry Router over an enterprise Wi-Fi network

Wi-Fi® enabled BlackBerry® devices can open a direct connection to the BlackBerry Router over an enterprise Wi-Fi network after you configured a Wi-Fi profile for the user accounts. You can use direct connections to the BlackBerry Router when Wi-Fi enabled BlackBerry devices are located in your organization's existing Wi-Fi environment. When BlackBerry devices connect to the BlackBerry Router, they can bypass SRP connectivity and authentication to connect to the BlackBerry® Enterprise Server directly.

After BlackBerry devices connect to the Wi-Fi network using a Wi-Fi profile, the BlackBerry devices try to make a direct IP connection to the BlackBerry Router. With some network architectures, a VPN session might be required to complete the direct connection to the BlackBerry Router.

Wi-Fi enabled BlackBerry devices include a built-in VPN client that you can configure and assign to any Wi-Fi profile on the BlackBerry devices. If a direct connection to the BlackBerry Router is possible (with or without a VPN session), the BlackBerry Enterprise Server starts sending data.

Wi-Fi connection when a VPN connection or direct connection between BlackBerry devices and the BlackBerry Router is not possible

If Wi-Fi® enabled BlackBerry® devices cannot connect directly to the BlackBerry Router (with or without a VPN connection) over a Wi-Fi network that can access the Internet (for example, a home Wi-Fi network or hotspot), the Wi-Fi enabled BlackBerry devices open SSL connections over the Internet to the BlackBerry® Infrastructure. After the Wi-Fi enabled BlackBerry devices connect to the BlackBerry Infrastructure, the users' provisioned data services start to send data to the Wi-Fi enabled BlackBerry devices.

Priority for connections that BlackBerry devices make over a Wi-Fi network

Wi-Fi® enabled BlackBerry® devices connect over a Wi-Fi network to the BlackBerry Router or BlackBerry® Infrastructure using the best possible connection or combination of available connections in the following order:

- connection to the BlackBerry® Enterprise Server or BlackBerry MDS Connection Service over a serial, USB, or Bluetooth® connection that uses the BlackBerry® Device Manager
- connection to the BlackBerry Router from a Wi-Fi network, with or without a VPN connection
- SSL connection through the Internet to the BlackBerry Infrastructure over a Wi-Fi network
- connection to the BlackBerry Infrastructure provided by a wireless service provider that uses the GSM® network, EDGE network, or UMA

The order of connections assumes that all routes to the BlackBerry Router and Internet are available when the Wi-Fi enabled BlackBerry devices connect to the Wi-Fi network.

BlackBerry services that are available over Wi-Fi connections

For more information about supported services and features, contact your organization's wireless service provider. Not all BlackBerry® data plans support Wi-Fi® access to BlackBerry data services.

When you configure a Wi-Fi network to open a connection (with or without a VPN connection) to the BlackBerry Router, you can keep all data transfers entirely within the enterprise Wi-Fi network and reduce the routing required.

BlackBerry services	Service provider with GSM®/EDGE network or UMA network	Wi-Fi network and service provider with GSM/EDGE network	Wi-Fi network and no service provider with GSM/EDGE network or UMA, and no UMA available	Enterprise Wi-Fi network and service provider with GSM/EDGE network, and no UMA, and no UMA available	Enterprise Wi-Fi network and no service provider with GSM/EDGE network, and no UMA available
services from the BlackBerry® Enterprise Server (for example, messaging, organizer data synchronization)	X	X	X	X	X

BlackBerry services	Service provider with GSM®/EDGE network or UMA network	Wi-Fi network and service provider with GSM/EDGE network	Wi-Fi network and no service provider with GSM/EDGE network or UMA, and no UMA available	Enterprise Wi-Fi network and service provider with GSM/EDGE network, and no UMA, and no UMA available	Enterprise Wi-Fi network and no service provider with GSM/EDGE network, and no UMA available
services from the BlackBerry® Internet Service (for example, messaging, browsing)	X	X	X	X	X
services from the BlackBerry MDS Connection Service (for example, application push, application access, browsing)	X	X	X	X	X
BlackBerry® Messenger	X	X	X	X	X
PIN messaging	X	X	X	X	X
instant messaging using a collaboration client (for example, Microsoft® Office Live Communications Server)	X	X	X	X	X

BlackBerry services	Service provider with GSM®/EDGE network or UMA network	Wi-Fi network and service provider with GSM/EDGE network	Wi-Fi network and no service provider with GSM/EDGE network or UMA, and no UMA available	Enterprise Wi-Fi network and service provider with GSM/EDGE network, and no UMA, and no UMA available	Enterprise Wi-Fi network and no service provider with GSM/EDGE network, and no UMA available
instant messaging using a third-party instant messaging application (for example, Windows® Messenger)	X	X	X	X	X
BlackBerry® Maps	X	X	X	X	X
service provider messaging (for example, SMS)	X	X		X	
content downloading provided by a wireless service provider (for example, ring tones)	X	X		X	
web browsing provided by a wireless service provider (for example, WAP)	X	X		X	
voice plan provided by a wireless service provider	X	X		X	

IEEE 802.11 wireless networking standards that Wi-Fi enabled BlackBerry devices support

Wi-Fi® enabled BlackBerry® devices support the IEEE® 802.11a, IEEE 802.11b, and IEEE 802.11g wireless networking standards.

Characteristics of the IEEE 802.11a wireless networking standard that Wi-Fi enabled BlackBerry devices support

Characteristic	Description
fallback speeds	48, 36, 24, 18, 12, 9, and 6 Mbps
frequency	5 GHz
maximum speed	54 Mbps
nonoverlapping channels	up to 19
sources of interference	• Bluetooth® wireless technology • some satellite systems • 5 GHz cordless phones
throughput speed	23 Mbps

Characteristics of the IEEE 802.11b wireless networking standard that Wi-Fi enabled BlackBerry devices support

Characteristic	Description
fallback speeds	5.5, 2, and 1 Mbps
frequency	2.4 GHz
maximum speed	11 Mbps
nonoverlapping channels	3
sources of interference	• Bluetooth® wireless technology • microwave ovens • 2.4 GHz cordless phones
throughput speed	4.5 Mbps

Characteristics of the IEEE 802.11g wireless networking standard that Wi-Fi enabled BlackBerry devices support

Characteristic	Description
fallback speeds	48, 36, 24, 18, 12, 9, and 6 Mbps
frequency	2.4 GHz
maximum speed	54 Mbps
nonoverlapping channels	3
sources of interference	• Bluetooth® wireless technology • microwave ovens • 2.4 GHz cordless phones
throughput speed	19 Mbps

Glossary

7

AES
Advanced Encryption Standard

AJAX
Asynchronous JavaScript® and XML

API
application programming interface

ASCII
American Standard Code for Information Interchange

BlackBerry Client Access License
A BlackBerry® Client Access License (BlackBerry CAL) limits how many users you can add to a BlackBerry® Enterprise Server.

BlackBerry Domain
A BlackBerry Domain consists of the BlackBerry Configuration Database with its users and any BlackBerry® Enterprise Server instances that connect to it.

BlackBerry MDS
BlackBerry® Mobile Data System

CBC
cipher block chaining

CMIME
Compressed Multipurpose Internet Mail Extensions

DES
Data Encryption Standard

DMZ
A demilitarized zone (DMZ) is a neutral subnetwork outside of an organization's firewall. It exists between the trusted LAN of the organization and the untrusted external wireless network and public Internet.

DNS
A Domain Name System (DNS) is an Internet database that translates domain names that are meaningful and recognizable by people into the numeric IP addresses that the Internet uses.

DOM
Document Object Model

DRM
Digital Rights Management

ECC
Elliptic Curve Cryptography

EDGE
Enhanced Data Rates for Global Evolution

GAL
Global Address List

GAN
generic access network

GME
The gateway message envelope (GME) protocol is a Research In Motion proprietary protocol that allows the transfer of compressed and encrypted data between the wireless network and BlackBerry devices. The protocol defines a routing layer that specifies the types of message contents allowed and the addressing information for the data. Gateways and routing components use this information to identify the type and source of the BlackBerry device data, and the appropriate destination service to route the data to.

HTML
Hypertext Markup Language

HTTP
Hypertext Transfer Protocol

HTTPS
Hypertext Transfer Protocol over Secure Sockets Layer

ISP
Internet service provider

IP
Internet Protocol

IP address
An Internet Protocol (IP) address is an identification number that each computer or mobile device uses when it sends or receives information over a network, such as the Internet. This identification number identifies the specific computer or mobile device on the network.

Java ME
Java® Platform, Micro Edition

JSON
JavaScript® Object Notation

LAN
A local area network (LAN) is a computer network shared by a group of computers in a small area, such as an office building. Any computer in this network can communicate with another computer that is part of the same network.

LTPA
Lightweight Third-Party Authentication

messaging server
A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.

MTLS
Mutual Transport Layer Security

NAT
network address translation

NTLM
NT LAN Manager

PAC
proxy auto-configuration

PIN
personal identification number

PKI
Public Key Infrastructure

RTF
Rich Text Format

SIM
Subscriber Identity Module

S/MIME
Secure Multipurpose Internet Mail Extensions

SMS
Short Message Service

SNMP

Simple Network Management Protocol

SQL
Structured Query Language

SRP
Server Routing Protocol

SSL
Secure Sockets Layer

TCP/IP
Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of communication protocols that is used to transmit data over networks, such as the Internet.

Triple DES
Triple Data Encryption Standard

UCS
Universal Content Stream

UMA
Unlicensed Mobile Access

UNC
Universal Naming Convention

USB
Universal Serial Bus

VPN
virtual private network

WAP
Wireless Application Protocol

XML
Extensible Markup Language

Provide feedback

8

To provide feedback on this deliverable, visit www.blackberry.com/docsfeedback.

Legal notice

9

©2009 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated. Bluetooth is a trademark of Bluetooth SIG. Corel and WordPerfect are trademarks of Corel Corporation. Eclipse is a trademark of Eclipse Foundation, Inc. GSM is a trademark of the GSM MOU Association. IBM, Lotus, and Sametime are trademarks of International Business Machines Corporation. IEEE is a trademark of the Institute of Electrical and Electronics Engineers, Inc. Java and JavaScript are trademarks of Sun Microsystems, Inc. Kerberos is a trademark of the Massachusetts Institute of Technology. Microsoft, ActiveX, Excel, Outlook, PowerPoint, SQL Server, Visual Studio, Windows Server and Windows are trademarks of Microsoft Corporation. Novell and GroupWise are trademarks of Novell, Inc. Open Mobile Alliance is a trademark of Open Mobile Alliance Ltd. PGP is a trademark of PGP Corporation. RSA SecurID is a trademark of RSA Security. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

The BlackBerry smartphone and other devices and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in the U.S. and in various countries around the world. Visit www.rim.com/patents for a list of RIM (as hereinafter defined) patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE

HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation

thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Certain features outlined in this documentation might require additional development or Third Party Products and Services for access to corporate applications.

This product contains a modified version of HTML Tidy. Copyright © 1998-2003 World Wide Web Consortium (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All Rights Reserved.

This product includes software developed by the Apache Software Foundation (www.apache.org/) and/or is licensed pursuant to one of the licenses listed at (www.apache.org/licenses/). For more information, see the NOTICE.txt file included with the software.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House
36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada